

JP2002335273

Title:

**METHOD, SYSTEM AND PROGRAM FOR PERFORMING REMOTE
MAINTENANCE AND RECORDING MEDIUM FOR RECORDING THE REMOTE
MAINTENANCE PERFORMANCE PROGRAM**

Abstract.

PROBLEM TO BE SOLVED: To provide a method, program and system for performing remote maintenance capable of remote maintenance on a plurality of Internet gateway terminals and their extension terminals to the utmost at the same time by way of a VPN (Virtual Private Network) on the Internet from a maintenance center while permitting duplicate local network addresses under the control, and to provide a recording medium for recording the remote maintenance execution program. **SOLUTION:** The method, program and system for executing remote maintenance adopts a characteristic configuration method realized such that a NAT(network address translation) 110 leading to a local network 7 is provided in a router section 11 in the Internet gateway terminal 1 to convert a global address into a local IP address for VPN NAT thereby allowing the maintenance center 9 to provide/release it.

(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2002-335273

(P2002-335273A)

(43) 公開日 平成14年11月22日 (2002. 11. 22)

(51) Int.Cl.⁷

H 0 4 L 12/56

12/46

識別記号

F I

H 0 4 L 12/56

12/46

テーマコード(参考)

H 5 K 0 3 0

B 5 K 0 3 3

A

審査請求 未請求 請求項の数25 O L (全 54 頁)

(21) 出願番号 特願2001-350783(P2001-350783)

(22) 出願日 平成13年11月15日(2001. 11. 15)

(31) 優先権主張番号 特願2001-63453(P2001-63453)

(32) 優先日 平成13年3月7日(2001. 3. 7)

(33) 優先権主張国 日本 (J P)

(71) 出願人 000004226

日本電信電話株式会社

東京都千代田区大手町二丁目3番1号

(72) 発明者 中濱 清志

東京都千代田区大手町二丁目3番1号

日本電信電話株式会社内

(72) 発明者 山田 敬信

東京都千代田区大手町二丁目3番1号

日本電信電話株式会社内

(74) 代理人 100071113

弁理士 菅 隆彦

Fターム(参考) 5K030 HA08 HD03 MA01 MD00

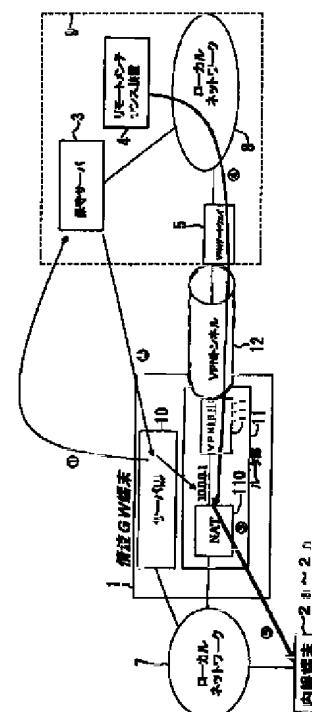
5K033 CB09 EC00

(54) 【発明の名称】 リモートメンテナンス実施方法、システム及びプログラム並びにリモートメンテナンス実施プログラムを記録した記録媒体

(57) 【要約】

【課題】 保守センタからインターネットのVPN経由で、配下のローカルネットワークアドレスの重複を許容した複数の情流GW端末及びその内線端末に対して、同時に可能な限りリモートメンテナンスできる、リモートメンテナンス実施方法、プログラム及びシステム並びにリモートメンテナンス実施プログラムを記録した記録媒体の提供。

【解決手段】 情流GW端末1におけるルータ部11内に、そのローカルネットワーク7との間にNAT110を設け、グローバル側のアドレスをVPN NAT用ローカルIPアドレスとして保守センタ9から付与及び解放を行うことで実現する特徴的構成手法の採用。



【特許請求の範囲】

【請求項1】各ローカルネットワークにより任意数の内線端末とIP接続してそれぞれのインターネットゲートウェイ端末の支配下とする一方、当該それぞれのインターネットゲートウェイ端末とインターネットを介してVPNゲートウェイ間でOSI参照モデルのネットワーク層においてVPNセッションを実現するIPsecを確立することにより、当該VPNゲートウェイを含む保守センタからリモートメンテナンスを行う実施方法であって、前記それぞれのインターネットゲートウェイ端末におけるルータ部内に、そのローカルネットワークとVPN処理部との間にVPN NATを設け、グローバル側のアドレスをVPN NAT用ローカルIPアドレスとして前記保守センタの保守サーバから付与及び解放を行うことにより前記リモートメンテナンスを実施する、ことを特徴とするリモートメンテナンス実施方法。

【請求項2】前記実施方法における前記リモートメンテナンスの要求は、当該要求を行う前記インターネットゲートウェイ端末が、リモートメンテナンス対象である内線端末名及び当該インターネットゲートウェイ端末のグローバルIPアドレスを、リモートメンテナンス要求コマンドとして前記保守サーバに通知すると、当該通知を受けた当該保守サーバが、当該通知したリモートメンテナンス対象の前記内線端末に付与するVPN NAT用ローカルIPアドレス及び内線端末名を、当該通知をしてきたインターネットゲートウェイ端末にリモートメンテナンス要求レスポンスとしてレスポンスすると共に、当該インターネットゲートウェイ端末のグローバルIPアドレスとの間において設置通知の際に共有されるIPsecの認証鍵を用いたIPsecによるVPNトンネルの確立を自己のVPNゲートウェイに設定させ、当該VPNゲートウェイに対してVPN NAT用ローカルIPアドレス宛のパケットを前記確立したVPNトンネルのVPN処理対象パケットとする設定を行い、前記レスポンスを受けたインターネットゲートウェイ端末が、受けた前記内線端末名に対する実ローカルIPアドレスを取得して、当該内線端末名に対する実ローカルIPアドレスと前記VPN NAT用ローカルIPアドレスとを静的NATとし自己のルータ部に対して設定を行う、以上の一連の処理を順次実施する、ことを特徴とする請求項1に記載のリモートメンテナンス実施方法。

【請求項3】前記リモートメンテナンスの実施は、前記リモートメンテナンス対象である前記内線端末に対して、前記VPN NAT用ローカルIPアドレスで前記確立されたVPNトンネルを経由して、前記保守センタから行われる、

ことを特徴とする請求項2に記載のリモートメンテナンス実施方法。

【請求項4】前記リモートメンテナンスの終了は、まず、前記VPN NAT用ローカルIPアドレスで前記確立されたVPNトンネルを経由して、当該VPNトンネルを確立させた前記インターネットゲートウェイ端末のサーバ部に対して、リモートメンテナンス終了コマンドを送信し、次に、当該送信を受けたサーバ部において、当該リモートメンテナンス終了コマンドに係る処理を行い、リモートメンテナンス終了レスポンスを送信し、その後、当該リモートメンテナンス終了レスポンスを受信した保守サーバにて、該当内線端末に対するメンテナンスが全て終了したかの第1判断を行い、当該第1判断にて肯定の場合には当該終了した内線端末は前記インターネットゲートウェイ端末の前記サーバ部、前記ルータ部の何れかであるかの第2判断を行う一方、否定の場合には判断処理を終了し、当該第2判断にて否定の場合にはVPN NAT解放処理へ移行し、他方肯定の場合には対応する前記インターネットゲートウェイ端末に対するリモートメンテナンスを全て終了したかの第3判断を行い、当該第3判断にて肯定の場合にはVPN終了処理へ移行するとともに否定の場合には当該判断処理を終了する、以上の一連の処理を順次実施する、ことを特徴とする請求項2又は3に記載のリモートメンテナンス実施方法。

【請求項5】前記VPN NAT解放処理は、まず、前記保守サーバが、前記リモートメンテナンスの要求の際に設定した前記リモートメンテナンス対象の内線端末名に対するVPN NAT用ローカルIPアドレスを、前記確立したVPNトンネルへのVPN処理対象パケットから解除する一方で、前記インターネットゲートウェイ端末に対して当該リモートメンテナンス対象の内線端末名を通知した後に、当該通知を受けたインターネットゲートウェイ端末が、当該受けた内線端末名に対する実ローカルIPアドレスを取得して、それに対するVPN NAT用ローカルアドレスとの静的NATを解放し、引続き、前記保守サーバが、前記第3判断を行いその判断結果に従う、以上の一連の処理を順次実施する、ことを特徴とする請求項4に記載のリモートメンテナンス実施方法。

【請求項6】前記VPN終了処理は、前記保守サーバが、IPsecセッションの終了をVPN終了コマンドとして、前記インターネットゲートウェイ端末に通知して、当該通知を受けたインターネットゲートウェイ端末が、当該VPN終了コマンドに対する返答を当該保守サーバにVPN終了レスポンスとして送信し、

前記保守サーバが、前記VPNゲートウェイに、前記リモートメンテナンスの要求に際して設定した前記VPNトンネルを解除させ、当該VPNゲートウェイと前記インターネットゲートウェイ端末間で確立されているVPNトンネル処理を終了する、
 以上の一連の処理を順次実施する、
 ことを特徴とする請求項4又は5に記載のリモートメンテナンス実施方法。

【請求項7】前記設置通知は、
 新たに設置された前記インターネットゲートウェイ端末の前記サーバ部から、当該設置について前記保守サーバに設置通知コマンドを通知し、
 当該設置通知コマンドを受けた当該保守サーバにより、前記リモートメンテナンスのための共通情報であるIPsecの認証鍵を生成して、当該設置通知コマンドを通知してきた前記インターネットゲートウェイ端末にレスポンスし、
 当該レスポンスを受信した前記インターネットゲートウェイ端末は、IPsecの認証鍵を自己の前記ルータ部に対して設定する、
 以上の一連の処理を順次実施する、
 ことを特徴とする請求項2、3、4、5又は6に記載のリモートメンテナンス実施方法。

【請求項8】前記実施方法は、
 前記リモートメンテナンスの要求、前記設定通知の何れか一方において、前記インターネットゲートウェイ端末の前記サーバ部及び前記ルータ部へのVPN NAT設定処理を実施する、
 ことを特徴とする請求項2、3、4、5、6又は7に記載のリモートメンテナンス実施方法。

【請求項9】前記実施方法は、
 前記インターネットゲートウェイ端末に故障発生を検知した場合には、
 先ず、当該インターネットゲートウェイ端末が、故障通知コマンドとして故障に係る情報を前記保守サーバに送信し、
 次に、前記保守サーバが前記故障通知コマンドを受信すると当該故障に係る情報を処理して、当該故障通知コマンドを送信した前記インターネットゲートウェイ端末に故障通知レスポンスとして送信し、
 更に、当該故障通知レスポンスを受信した当該インターネットゲートウェイ端末が前記リモートメンテナンスの要求に移行する、
 以上の一連の処理を順次実施する、
 ことを特徴とする請求項2、3、4、5、6、7又は8に記載のリモートメンテナンス実施方法。

【請求項10】各ローカルネットワークにより任意数の内線端末とIP接続してそれぞれのインターネットゲートウェイ端末の支配下とする一方、当該それぞれのインターネットゲートウェイ端末とインターネットを介して

VPNゲートウェイ間でOS I参照モデルのネットワーク層においてVPNセッションを実現するIPsecを確立することで、当該VPNゲートウェイを含む保守センタからリモートメンテナンスを行うシステムであって、

前記インターネットゲートウェイ端末におけるルータ部にそのローカルネットワークとVPN処理部との間にNATを設け、グローバル側のアドレスをVPN NAT用ローカルIPアドレスとして前記保守センタから付与及び解放を行う機能構成にシステム構築する、
 ことを特徴とするリモートメンテナンス実施システム。

【請求項11】前記保守センタは、
 前記インターネットゲートウェイ端末からリモートメンテナンス対象の内線端末名の通知を受けて当該リモートメンテナンス対象の内線端末名に対応するVPNアクセス用のVPN NAT用ローカルアドレスの付与を行う保守サーバと、
 前記リモートメンテナンスを行うリモートメンテナンス装置と、

当該リモートメンテナンス装置からの、当該リモートメンテナンス対象の内線端末名に対応するVPN NAT用ローカルIPアドレスへアクセスを経由するVPNゲートウェイとを、
 保守センタローカルネットワークにてネットワーク構築する、
 ことを特徴とする請求項10に記載のリモートメンテナンス実施システム。

【請求項12】前記インターネットゲートウェイ端末は、
 前記保守センタにリモートメンテナンス対象の内線端末名を通知するサーバ部と、
 当該通知したことにより当該保守センタから付与されたVPNアクセス用のVPN NAT用ローカルIPアドレスと当該リモートメンテナンス対象の内線端末名のIPアドレスを割りつけるVPN NAT及び当該保守センタの前記VPNゲートウェイとVPNトンネルを確立するVPN処理部のルータ部とで構成して、
 前記VPNゲートウェイを介した、リモートメンテナンス対象端末名に対するVPN NAT用ローカルIPアドレスへのアクセスにより、前記リモートメンテナンスを行うリモートメンテナンス装置からの、前記内線端末へのパケット転送を可能ならしめる機能を構築する、
 ことを特徴とする請求項10又は11に記載のリモートメンテナンス実施システム。

【請求項13】各ローカルネットワークにより任意数の内線端末とIP接続してそれぞれのインターネットゲートウェイ端末の支配下とする一方、当該それぞれのインターネットゲートウェイ端末とインターネットを介してVPNゲートウェイ間でOS I参照モデルのネットワーク層においてVPNセッションを実現するIPsecを

確立することで、当該VPNゲートウェイを含む保守センタからリモートメンテナンスを行うシステムにおける、当該インターネットゲートウェイ端末で用いられるプログラムであって、

当該インターネットゲートウェイ端末が設置された後に、リモートメンテナンスサービスを利用する場合に、前記保守センタに対して設置した旨を通知する設置通知処理を当該インターネットゲートウェイ端末に行わせる前記プログラムの実行により、前記設置について前記保守センタの保守サーバに設置通知コマンドを通知した後に、当該保守サーバからの当該設置通知コマンドに対するレスポンスを受信すると当該レスポンスとして受けたIPsecの認証鍵を自己のルート部に対して設定する、
以上の一連の手順を踏む、ことを特徴とするリモートメンテナンス実施プログラム。

【請求項14】各ローカルネットワークにより任意数の内線端末とIP接続してそれぞれのインターネットゲートウェイ端末の支配下とする一方、当該それぞれのインターネットゲートウェイ端末とインターネットを介してVPNゲートウェイ間でOSI参照モデルのネットワーク層においてVPNセッションを実現するIPsecを確立することで、当該VPNゲートウェイを含む保守センタからリモートメンテナンスを行うシステムにおける、当該インターネットゲートウェイ端末にて用いられるプログラムであって、
当該インターネットゲートウェイ端末への、前記内部端末からのWEBアクセス、当該インターネットゲートウェイ端末の操作者によるボタン操作の何れかにより、リモートメンテナンスを要求するリモートメンテナンス要求処理を当該インターネットゲートウェイ端末に行わせる前記プログラムの実行により、
リモートメンテナンス対象である前記内線端末名及び前記インターネットゲートウェイ端末のグローバルIPアドレスを、リモートメンテナンス要求コマンドとして前記保守サーバに通知した後に、
前記リモートメンテナンス要求コマンドに対するレスポンスを受けて、当該レスポンスとして受けた、内線端末名に対する実ローカルIPアドレスを取得して、当該内線端末名に対する実ローカルIPアドレスと当該レスポンスとして受けたVPN NAT用ローカルIPアドレスとを静的NATとして設定させる、
以上の一連の手順を踏む、
ことを特徴とするリモートメンテナンス実施プログラム。

【請求項15】各ローカルネットワークにより任意数の内線端末とIP接続してそれぞれのインターネットゲートウェイ端末の支配下とする一方、当該それぞれのインターネットゲートウェイ端末とインターネットを介してVPNゲートウェイ間でOSI参照モデルのネットワー

ク層においてVPNセッションを実現するIPsecを確立することで、当該VPNゲートウェイを含む保守センタからリモートメンテナンスを行うシステムにおける、当該インターネットゲートウェイ端末にて用いられるプログラムであって、

前記保守センタより行われる前記リモートメンテナンスの作業が終了した旨の通知に係るリモートメンテナンス終了処理を、当該通知を受けた前記インフェースゲートウェイ端末に行わせる前記プログラムの実行により、
前記保守センタからのリモートメンテナンス終了コマンドの受信を契機に、当該リモートメンテナンス終了コマンドに関する処理を行い、リモートメンテナンス終了レスポンスを送信して、

前記保守センタからVPN解放コマンドとしてリモートメンテナンス対象の内線端末名の通知を受けた場合には、当該受けた内線端末名に対する実ローカルIPアドレスを取得し、取得した実ローカルIPアドレスに対するVPN NAT用ローカルアドレスとの静的NATを解放する、
以上の一連の手順を踏む、
ことを特徴とするリモートメンテナンス実施プログラム。

【請求項16】各ローカルネットワークにより任意数の内線端末とIP接続してそれぞれのインターネットゲートウェイ端末の支配下とする一方、当該それぞれのインターネットゲートウェイ端末とインターネットを介してVPNゲートウェイ間でOSI参照モデルのネットワーク層においてVPNセッションを実現するIPsecを確立することで、当該VPNゲートウェイを含む保守センタからリモートメンテナンスを行うシステムにおいて、当該保守センタにて用いられるプログラムであって、

前記リモートメンテナンスの要求に対応するリモートメンテナンス要求処理を前記保守サーバに行わせる前記プログラムの実行により、
前記要求を受けて、前記リモートメンテナンスの要求に係るリモートメンテナンス対象の前記内線端末に付与するVPN NAT用ローカルIPアドレス及び内線端末名を、当該要求を行った前記インターネットゲートウェイ端末にリモートメンテナンス要求レスポンスとして送信すると共に、当該インターネットゲートウェイ端末のグローバルIPアドレスとの間において共有されるIPsecの認証鍵を用いたIPsecによるVPNトンネルの確立を、自己のVPNゲートウェイに指示し、自己の当該VPNゲートウェイに対して、VPN NAT用ローカルIPアドレス宛のパケットを、当該指示により確立されるVPNトンネルのVPN処理対象パケットとする設定を行う、
以上の一連の手順を踏む、ことを特徴とするリモートメンテナンス実施プログラム。

【請求項17】各ローカルネットワークにより任意数の内線端末とIP接続してそれぞれのインターネットゲートウェイ端末の支配下とする一方、当該それぞれのインターネットゲートウェイ端末とインターネットを介してVPNゲートウェイ間でOSI参照モデルのネットワーク層においてVPNセッションを実現するIPsecを確立することで、当該VPNゲートウェイを含む保守センタからリモートメンテナンスを行うシステムにて、当該保守センタにて用いられるプログラムであって、新たに設置された前記インターネットゲートウェイ端末からの設置通知コマンドを処理する設定通知コマンド処理を前記保守センタに行わせる前記プログラムの実行により、前記設置通知コマンドに応じて、前記リモートメンテナンスのための共通情報であるIPsecの認証鍵を生成して、当該設置通知コマンドを通知してきた前記インターネットゲートウェイ端末にレスポンスする、以上の一連の手順を踏む、ことを特徴とするリモートメンテナンス実施プログラム。

【請求項18】各ローカルネットワークにより任意数の内線端末とIP接続してそれぞれのインターネットゲートウェイ端末の支配下とする一方、当該それぞれのインターネットゲートウェイ端末とインターネットを介してVPNゲートウェイ間でOSI参照モデルのネットワーク層においてVPNセッションを実現するIPsecを確立することで、当該VPNゲートウェイを含む単一の保守センタからリモートメンテナンスを行うシステムにおいて、当該保守センタにて用いられるプログラムであって、前記保守センタにおける終了ボタンが押されたことを契機に、前記リモートメンテナンスの作業が終了したことを通知するリモートメンテナンス終了処理を、前記保守サーバに行わせる前記プログラムの実行により、VPN NAT用ローカルIPアドレスで確立されたVPNトンネルを経由して、当該VPNトンネルを確立させた前記インターネットゲートウェイ端末のサーバ部に対して、リモートメンテナンス終了コマンドを送信した後に、当該リモートメンテナンス終了のレスポンスを受信すると、該当内線端末に対するメンテナンスが全て終了したかの第1判断を行い、当該第1判断にて肯定の場合には当該終了した前記内線端末は前記インターネットゲートウェイ端末の前記サーバ部かルータ部かの何れかであるかの第2判断を行う一方、否定の場合にはこのプログラムを終了し、当該第2判断にて否定の場合にはVPN NAT解放処理へ移行する一方、肯定の場合には対応する前記インターネットゲートウェイ端末に対するリモートメンテナンスを全て終了したかの第3判断を行い、

当該第3判断にて肯定の場合にはVPN終了処理へ移行する一方、否定の場合にはこのプログラムを終了する、以上の一連の手順を踏む、ことを特徴とするリモートメンテナンス実施プログラム。

【請求項19】前記VPN NAT解放処理は、リモートメンテナンス要求を受けて設定したリモートメンテナンス対象の内線端末名に対するVPN NAT用ローカルIPアドレスを、確立した前記VPNトンネルへのVPN処理対象バケットから解除する様、前記VPNゲートウェイに対して行い、前記インターネットゲートウェイ端末に対して、リモートメンテナンス対象の内線端末名を通知し、その後、前記第3判断にリターンする一連の処理であり、前記VPN終了処理は、

IPsecセッションの終了をVPN終了コマンドとして、前記インターネットゲートウェイ端末に対して送信して、前記VPNゲートウェイに、リモートメンテナンス実施要求の際に設定した前記VPNトンネルの解除させ、当該VPNゲートウェイと当該インターネットゲートウェイ端末間で確立されているVPNトンネル処理を終了させる一連の処理である、ことを特徴とする請求項18に記載のリモートメンテナンス実施プログラム。

【請求項20】請求項13、14、15、16、17、18又は19に記載のリモートメンテナンス実施プログラムによる一連の手続を実録した、ことを特徴とするリモートメンテナンス実施プログラムを記録した記録媒体。

【請求項21】インターネットに接続された複数のインターネットゲートウェイ端末自体及びその配下のローカルネットワークにIP接続された内線端末を、当該インターネットゲートウェイ端末と当該インターネットに接続されたVPNゲートウェイ間でOSI参照モデルのネットワーク層においてVPNセッションを実現するIPsecを確立することにより、当該VPNゲートウェイ配下の単一の保守サーバからリモートメンテナンスを行う実施方法であって、VPNを構築する前に、前記インターネットゲートウェイ端末からのVPN構築要求を受けた前記保守センタが、その配下の複数のVPNゲートウェイからVPNの空きリソースのあるVPNゲートウェイを動的に選択して、当該選択されたVPNゲートウェイのグローバルIPアドレスを当該インターネットゲートウェイ端末に通知し、当該インターネットゲートウェイ端末は当該通知されたグローバルIPアドレスを当該VPNの対向ホストとして設定を行うことにより、前記リモートメンテナンスを実施する、ことを特徴とするリモートメンテナンス実施方法。

【請求項22】インターネットに接続された複数のイン

ターネットゲートウェイ端末自体及びその配下のローカルネットワークにIP接続された内線端末を、当該インターネットゲートウェイ端末と当該インターネットに接続されたVPNゲートウェイ間でOS I参照モデルのネットワーク層においてVPNセッションを実現するIPsecを確立することにより、当該VPNゲートウェイ配下の単一の保守サーバからリモートメンテナンスを行うシステムであって、

前記インターネットゲートウェイ端末からVPN構築の要求を受けると、その配下の複数のVPNゲートウェイからVPNの空きリソースのあるVPNゲートウェイを動的に選択して、当該選択されたVPNゲートウェイのグローバルIPアドレスを、当該要求をなしたインターネットゲートウェイ端末に通知する前記保守センタと、当該保守センタに対して前記VPN構築の要求を行うと共に、当該要求に対する当該保守センタから前記通知された前記選択されたVPNゲートウェイのグローバルIPアドレスを、当該VPNの対向ホストとして設定する前記インターネットゲートウェイ端末と、

を具備する、

ことを特徴とするリモートメンテナンス実施システム。

【請求項23】インターネットに接続された複数のインターネットゲートウェイ端末自体及びその配下のローカルネットワークにIP接続された内線端末を、当該インターネットゲートウェイ端末と当該インターネットに接続されたVPNゲートウェイ間でOS I参照モデルのネットワーク層においてVPNセッションを実現するIPsecを確立することにより、当該VPNゲートウェイ配下の単一の保守サーバからリモートメンテナンスを行うシステムにおける、当該インターネットゲートウェイ端末にて用いられるプログラムであって、

前記内線端末からのリモートメンテナンス要求の登録又はインターネットゲートウェイ端末管理者による前記インターネットゲートウェイ端末本体のボタン操作の何れかにより、VPNゲートウェイアドレスを要求するVPNゲートウェイアドレス要求処理を当該インターネットゲートウェイ端末に行わせる前記プログラムの実行により、

前記保守センタに対して前記VPNゲートウェイアドレスの要求を行うと共に、

当該保守センタから当該要求に対するVPNゲートウェイアドレス要求レスポンスを受信すると、当該VPNゲートウェイアドレス要求レスポンスとして受信したVPNゲートウェイグローバルIPアドレスを、VPNの対向ホストとして、自己のルータ部に設定して、前記リモートメンテナンス要求の処理を行う、以上の一連の手順を踏む、

ことを特徴とするリモートメンテナンス実施プログラム。

【請求項24】インターネットに接続された複数のイン

ターネットゲートウェイ端末自体及びその配下のローカルネットワークにIP接続された内線端末を、当該インターネットゲートウェイ端末とインターネットに接続されたVPNゲートウェイ間でOS I参照モデルのネットワーク層においてVPNセッションを実現するIPsecを確立することにより、当該VPNゲートウェイ配下の単一の保守サーバからリモートメンテナンスを行うシステムにおける、当該保守センタにて用いられるプログラムであって、

前記インターネットゲートウェイ端末からのVPNゲートウェイアドレス要求に伴う前記保守センタ内の処理であるVPNゲートウェイアドレス要求処理を当該保守センタに行わせる前記プログラムの実行により、

前記インターネットゲートウェイ端末から前記VPNゲートウェイアドレス要求を受信すると、自己の支配下の複数のVPNゲートウェイからVPN空きリソースのあるVPNゲートウェイを動的に選択し、そのVPNゲートウェイのグローバルIPアドレスを、当該VPNゲートウェイアドレス要求をなしたインターネットゲートウェイ端末に通知する、

以上の一連の手順を踏む、

ことを特徴とするリモートメンテナンス実施プログラム。

【請求項25】請求項23又は24に記載のリモートメンテナンス実施プログラムによる一連の手続を実録した、

ことを特徴とするリモートメンテナンス実施プログラムを記録した記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、インターネットに接続された保守センタからインターネットゲートウェイ端末自体及びそのインターネットゲートウェイ端末配下のローカルネットワークに接続されたパソコン等の内線端末をインターネット経由でVPNを利用してリモートメンテナンスを行うリモートメンテナンス実施方法、その実施に直接使用するリモートメンテナンスシステム、プログラム及び同記録媒体に関するものである。

【0002】

【従来の技術】従来、インターネットに接続された保守センタからインターネットゲートウェイ端末（以下、情流GW端末）自体及びその情流GW端末に接続されたローカルネットワーク上のパソコン（以下、内線端末）をインターネット経由でVPNを利用してリモートメンテナンスを行うリモートメンテナンス実施方法（以下、VPNリモートメンテナンスと呼ぶ）として、特願平2000-000496で提案されている方法がある。

【0003】しかし、特願平2000-000496の方法で提案されているVPNリモートメンテナンスでは、複数の情流GW端末に対して同時にリモートメンテ

ナンスを行う際、対象となる情流GW端末配下のローカルネットワークアドレスが重複している場合、保守センタからVPN経由でリモートメンテナンス対象の情流GW端末及びその配下の内線端末にパケットを送るとき、対象ローカルIPアドレスがバッティングするため、保守センタ側のVPNゲートウェイでは、どちらのローカルネットワークへパケットを送出してよいか判断できず、同時に同じローカルネットワークアドレスを持つ複数の情流GWへのメンテナンスを行うことが不可能であった。

【0004】そこで、保守センタのローカルネットワーク内から、配下に同じローカルネットワークアドレスを持つ複数の情流GWへ同時にメンテナンスを行う方法として、インターネット側から各々の情流GWの内部ネットワークを見たときにそのローカルネットワークアドレスがユニークになるようにする手法が考えられる。

【0005】具体的には、情流GWの内部に、保守センタ側とVPN通信するための仮のローカルネットワークアドレス（以下、VPN NAT用IPアドレス）とローカルネットワークアドレスを固定して結びつける処理部（以下、NATBOX）を設けるという手法であり、図32を元に動作を説明する。

【0006】図32において、クライアントPC（a）からサーバPC（b）へVPN NAT経由でIP通信を行う場合の、パケットのアドレスの変化を示すために、まず、各ノードの接続形態を説明する。クライアントPC（a）は、プライベートネットワーク（c）に接続されており192.168.2.103のプライベートIPアドレスを持つ。VPNゲートウェイ（d）は、プライベートネットワーク（c）に接続されており、インターネット（e）側のグローバルIPアドレスとして211.0.0.1を持つ。

【0007】VPNルータ（f）は、プライベートネットワーク（g）に接続されており、インターネット側のグローバルIPアドレスとして210.0.0.1を持つ。サーバPC（b）はプライベートネットワーク（c）に接続されており、192.168.1.1～192.168.1.254のプライベートIPアドレスを持つ。

【0008】また、VPNゲートウェイ（d）と情流GW（以下、VPNルータとも呼ぶ）は、VPNのトンネル（h）を構築している。VPNゲートウェイ（d）ではVPNルータ（b）へのVPNトンネル（h）に対してのVPN対象パケットとして10.0.0.0/24が設定されており、VPNルータ（b）では、VPNゲートウェイ（d）へのVPNトンネル（h）に対してのVPN対象パケットとして192.168.2.0/24が設定されている。

【0009】また、NATBOX（f10）は、インターネット（e）側にVPN NAT用IPアドレスとして10.0.0.1～10.0.0.254のアドレスを持ち、10.0.0.1と192.168.1.1、10.0.0.2と192.168.1.2、…（省略）、…、

10.0.0.254と192.168.1.254で静的NATが設定されている。

【0010】ここで、192.168.1.1のサーバPC（b）について着目すると、NATBOX（f10）のプライベートネットワーク（g）側から送信元アドレス192.168.1.1のパケットが送出される際は送信元アドレスが10.0.0.1に書き換えられてNATBOX（f10）のインターネット側へ送出され、NATBOX（f10）のインターネット（e）側から送信先10.0.0.1宛てのパケットが到着すると、送信先アドレスが192.168.1.1に書き換えられてNATBOX（f10）のプライベートネットワーク（c）側に送出される。

【0011】以下、クライアントPC（a）とサーバPC（b）間で通信を行う際のパケットのアドレス変化を示す。ここで、クライアントPC（a）からサーバPC（b）宛てのオリジナルパケットは、「送信元192.168.2.103：送信先10.0.0.1」で送出され、VPNゲートウェイ（d）に到着する。

【0012】VPNゲートウェイ（d）は、10.0.0.1のパケットを受信したのでVPNルータ（f）へのVPNトンネル（h）に対してのVPN対象パケットと判断し、「送信元211.0.0.1：送信先210.0.0.1」の新IPヘッダを付加し、カプセル化を行う。オリジナルパケットは暗号化されてデータ部に入る。このパケットは、VPNトンネルを経由してVPNルータのVPN処理部（f11）に到達する。

【0013】VPNルータのVPN処理部（f11）では、オリジナルパケットが復号化され、「送信元192.168.2.103：送信先10.0.0.1」としてNATBOX（f10）に送出する。NATBOX（f10）では、外側10.0.0.1と内側192.168.1.1で静的NATが設定されており、送信先アドレスが10.0.0.1にマッチするので、アドレス変換が行われ、「送信元192.168.2.103：送信先192.168.1.1」となり、プライベートネットワーク（c）のネットワークに送出される。したがって、このパケットは、サーバPC（b）に到着することができる。

【0014】また、サーバPC（b）からクライアントPC（a）へのレスポンスオリジナルパケットは、「送信元192.168.1.1：送信先192.168.2.103」で送出され、VPNルータ（f）に到着する。VPNルータ（f）では、192.168.2.0/24のパケットを受信したのでVPNゲートウェイ（d）へのVPNトンネル（h）に対してのVPN対象パケットと判断し、まずNATBOX（f10）にパケットが送られる。

【0015】NATBOX（f10）では、外側10.0.0.1と内側192.168.1.1で静的NATが設定されており、送信元アドレスが192.168.1.1にマッチするので、アドレス変換が行われ「送信元10.0.0.1：送信先192.168.2.103」となり、VPN処理部（b11）へ送られる。

【0016】VPN処理部（f11）では「送信元210.

0.0.1:送信先211.0.0.1」となり新IPヘッダを付加し、カプセル化を行う。レスポンスオリジナルパケットは暗号化されてデータ部に入る。このパケットは、VPNトンネル(h)を経由してVPNゲートウェイ(d)に到達する。VPNゲートウェイ(d)では、レスポンスオリジナルパケットが復号化され、「送信元10.0.0.1:送信先192.168.2.103」となり、プライベートネットワーク(c)のネットワークに送出される。したがって、このパケットは、クライアントPC(a)に到着することができる。

【0017】以上、保守センタから情流GW(f)1台で配下のローカルネットワークが1つの場合について保守センタのプライベートネットワーク(g)と情流GW(f)配下のプライベートネットワーク(c)を静的VPNNAT機能を適用して通信を行った場合の動作概要について説明した。なお、図中(f1)はNATBOX(f10)とVPN処理部(f11)で構成されるルータ部である。

【0018】次に、保守センタから情流GW(f')(f'')2台の配下のプライベートネットワーク(g')(g'')が2つあり、そのプライベートネットワークアドレスが重複している場合について、保守センタのプライベートネットワーク(c)から各々の情流GW(f')(f'')配下のプライベートネットワーク(g')(g'')に対して静的VPNNAT機能を適用して通信を行う場合の動作概要について説明する。

【0019】図33に情流GW(f')(f'')2台の配下のプライベートネットワークネットワークアドレスが同じケースにおいて、静的VPNNAT機能を用いて保守センタから2つの情流GW(f')(f'')配下のアドレスのサーバPC(b1)～(b4)に同時にアクセスする方法を示す。

【0020】ここで、クライアントPC(a)からサーバPC(b1)～(b4)へVPNNAT経由でIP通信を行う場合の、パケットのアドレスの変化を示すために、まず、各ノードの接続形態を説明する。クライアントPC(a)は、プライベートネットワーク(g')(g'')に接続されており192.168.2.103のプライベートIPアドレスを持つ。VPNゲートウェイ(d)は、プライベートネットワーク(c)に接続されており、インターネット(e)側のグローバルIPアドレスとして211.0.0.1を持つ。

【0021】VPNルータ(f')は、プライベートネットワーク(g')に接続されており、インターネット(e)側のグローバルIPアドレスとして210.0.0.1を持つ。サーバPC(b1)(b2)はVPNルータ(f')の内部ローカルネットワーク192.168.1.0/24に接続されており、192.168.1.1～192.168.1.254のプライベートIPアドレスを持つ。また、VPNゲートウェイ(d)とVPNルータ(f')は、VPNのトンネル

(h')を構築している。

【0022】VPNゲートウェイ(d)ではVPNルータ(f')へのVPNトンネル(h')に対してのVPN対象パケットとして10.0.0.0/24が設定されており、VPNルータ(f')では、VPNゲートウェイ(d)へのVPNトンネル(h')に対してのVPN対象パケットとして192.168.2.0/24が設定されている。

【0023】また、NATBOX(f10')は、インターネット(e)側にVPNNAT用IPアドレスとして10.0.0.1～10.0.0.254のアドレスを持ち、10.0.0.1と192.168.1.1、10.0.0.2と192.168.1.2、…、(省略)、…、10.0.0.254と192.168.1.254で静的NATが設定されている。

【0024】ここで、192.168.1.1のサーバPC(b1)(b2)について着目すると、NATBOX(f10)のプライベートネットワーク(g')側から送信元アドレス192.168.1.1のパケットが送出される際は送信元アドレスが10.0.0.1に書き換えられてNATBOX(f10')のインターネット側へ送出され、NATBOX(f10')のインターネット(e)側から送信先10.0.0.1宛てのパケットが到着すると、送信先アドレスが192.168.1.1に書き換えられてNATBOX(f')のプライベートネットワーク側に送出される。

【0025】VPNルータ(f'')は、プライベートネットワーク(g'')に接続されており、インターネット(e)側のグローバルIPアドレスとして210.0.1.1を持つ。サーバPC(b3)(b4)はVPNルータ(f'')の内部ローカルネットワーク192.168.1.0/24に接続されており、192.168.1.1～192.168.1.254のプライベートIPアドレスを持つ。

【0026】また、VPNゲートウェイ(d)とVPNルータ(f'')は、VPNのトンネル(h'')を構築している。VPNゲートウェイ(d)ではVPNルータ(f'')へのVPNトンネル(h'')に対してのVPN対象パケットとして10.0.1.0/24が設定されており、VPNルータ(f'')では、VPNゲートウェイ(d)へのVPNトンネル(h'')に対してのVPN対象パケットとして192.168.2.0/24が設定されている。

【0027】また、NATBOX(f10'')は、インターネット(e)側にVPNNAT用IPアドレスとして10.0.1.1～10.0.1.254のアドレスを持ち、10.0.1.1と192.168.1.1、10.0.1.2と192.168.1.2、…、(省略)、…、10.0.1.254と192.168.1.254で静的NATが設定されている。

【0028】ここで、192.168.1.1のサーバPC(b3)について着目すると、NATBOX(f'')のプライベートネットワーク(g'')側から送信元アドレス192.168.1.1のパケットが送出される際は送信元アドレスが10.0.1.1に書き換えられてNATBOX(f'')のインターネット(e)側へ送出され、NATBOX(f'')のイン

ターネット (e) 側から送信先10.0.1.1宛でのパケットが到着すると、送信先アドレスが192.168.1.1に書き換えられてNATBOX (f'') のプライベートネットワーク (g'') 側に送出される。

【0029】以上、保守センタから情流GW (f') (f'') 2台の配下のプライベートネットワーク (g') (g'') が2つあり、そのプライベートネットワークアドレスが重複している場合について、保守センタのプライベートネットワーク (c) から各々の情流GW (f') (f'') 配下のプライベートネットワーク (g') (g'') に対して静的VPN NAT機能を適用して通信を行う場合の動作概要について説明した。

【0030】言うまでもないが、前記示した「情流GW 2台の配下のプライベートネットワークが2つあり、そのプライベートネットワークアドレスが重複している場合」の動作は、「情流GWN (Nは任意の自然数) 台の配下のプライベートネットワークがN個あり、そのプライベートネットワークアドレスが重複している場合」にも適用できる。

【0031】従って、図33に示す方法で、静的VPN NATを構築した上で保守センタからアクセスすることにより、複数の情流GW端末 (VPNルータ) に対して同時にリモートメンテナンスを行う際、対象となる情流GW端末配下のプライベートネットワークアドレスが重複している場合でも、保守センタからVPN経由でリモートメンテナンス対象の情流GW端末及びその配下の内線端末 (サーバPC) にパケットを送るとき、対象プライベートIPアドレスを静的VPN NATで割り付けたNATBOXのインターネット側のアドレス向けに送出することにより、保守センタ側のVPNゲートウェイでは、どちらのプライベートネットワークへパケットを送出してよいか判断でき、同時に同じプライベートネットワークアドレスを持つ複数の情流GW端末へのメンテナンスを行うことが可能となる。以下、これを「静的VPN NAT方式」と呼ぶことにする。

【0032】また、特願平2000-000496にて提案されているVPNリモートメンテナンスでは、保守センタのVPNゲートウェイのグローバルIPアドレスを情流GW端末が事前に知っていることを必須とし、その対応策として、事前に情流GW端末にVPNゲートウェイのグローバルIPアドレスを埋め込んで出荷するという方法が採られていた。

【0033】

【発明が解決しようとする課題】しかし、前記説明した「静的VPN NAT」方式により保守センタのプライベートネットワークから情流GW端末配下の全てのプライベートネットワークに対してアクセスする場合は、情流GW端末とVPNゲートウェイ間でVPNを構築する時点で、情流GW端末においてVPN NAT用IPアドレスとプライベートネットワークの実ローカルIPアドレ

スを事前に静的VPN NATで割り付けておく必要があった。

【0034】この場合、保守センタ側がユニークに管理するVPN NAT用IPアドレスリソース (プライベートIPアドレス) を保守対象の情流GW端末配下のプライベートネットワークの端末台数分だけ事前に割り当てる必要があり、実際にメンテナンスを行う対象端末数に対して、非常に膨大な数のVPN NAT用IPアドレスリソースを必要とした。すなわち静的VPN NAT方式では、同クラスのプライベートIPアドレスを使った場合、最大約1670万台の情流GW端末配下の内線端末だけがリモートメンテナンス対象端末であった。

【0035】例えば、同クラスのプライベートアドレスをVPN NAT用IPアドレスリソースとして利用し、情流GW端末配下のプライベートネットワークのサブネットマスクが全て24ビットだった場合は最大約6万5千加入情流GW端末配下のプライベートネットワークのサブネットマスクが全て16ビットだった場合は最大約256加入の情流GW端末配下の端末しかメンテナンス対象とできないという制約事項があった。

【0036】また、静的VPN NAT方式を使って、特願平2000-000496の方法で提案されているVPNリモートメンテナンスを行う場合は、リモートメンテナンス要求をあげた情流GW端末配下の全ての内線端末リソースに保守センタからアクセスが可能となってしまおうという問題点があった。

【0037】また、VPNリモートメンテナンスの設置通知数が増大し、VPNリモートメンテナンスサービスの同時利用者がVPNゲートウェイの許容VPNセッション数を超える場合、保守センタ側でVPNゲートウェイを増設して設置する必要がある、その場合、VPNゲートウェイのグローバルIPアドレスを端末に設定させる手段が存在しなかった。また、保守センタのVPNゲートウェイアドレスを何らかの手段でインターネットゲートウェイ管理者に通知し、手動でVPNゲートウェイアドレスを設定させる方法は、リモートメンテナンスの際に人手が伴うので、VPNリモートメンテナンスには適用できないという問題点があった。

【0038】ここにおいて、本発明の解決すべき主要な目的は次の通りである。

【0039】本発明の第1の目的は、保守センタからインターネットのVPN経由で、配下のプライベート (ローカル) ネットワークアドレスの重複を許容した複数の情流GW端末及びその内線端末を同時にリモートメンテナンスする際、リモートメンテナンス対象の情流GW端末及び内線端末数の制限を、保守センタ側で管理するIPアドレスリソースの上限まで許容し、可能な限り多数の情流GW端末及びその配下の内線端末のリモートメンテナンスを同時に行うことを可能とするリモートメンテナンス実施方法、システム、プログラム及び記録媒体を

提供せんとするものである。

【0040】本発明の第2の目的は、保守センタ側がユニークに管理するVPN NAT要IPアドレスリソースを保守対象の情流GW端末配下のプライベートネットワークの端末台数分だけ事前に割り当てる必要のないリモートメンテナンス実施方法、システム、プログラム及び記録媒体を提供せんとするものである。

【0041】本発明の第3の目的は、VPNリモートメンテナンスを行う場合に、リモートメンテナンス要求をあげた情流GW端末配下のすべての内線端末リソースに保守センタからのアクセスが起らないようにしたリモートメンテナンス実施方法、システム、プログラム及び記録媒体を提供せんとするものである。

【0042】本発明の第4の目的は、VPNリモートメンテナンスの設置通知数が増大しVPNリモートメンテナンスの同時利用者が、VPNゲートウェイの許容VPNセッション数を超える場合、保守センタ側でVPNゲートウェイを増設して設置する必要があるが、その場合にVPNゲートウェイのグローバルIPアドレスを端末に設定するようにしたリモートメンテナンス実施方法、システム、プログラム及び記録媒体を提供せんとするものである。

【0043】本発明の他の目的は、明細書、図面、特に特許請求の範囲の各請求項の記載から自ずと明らかとなる。

【0044】

【課題を解決するための手段】本発明方法は、上記課題の解決に当たり、①各ローカルネットワークにより任意数の内線端末とIP接続してそれぞれのインターネットゲートウェイ端末の支配下とする一方、当該それぞれのインターネットゲートウェイ端末とインターネットを介してVPNゲートウェイ間でOS I参照モデルのネットワーク層においてVPNセッションを実現するIPsecを確立することで、当該VPNゲートウェイを含む単一の保守センタからリモートメンテナンスを行う実施方法であり、当該インターネットゲートウェイ端末におけるルータ部内に、その前記ローカルネットワークとVPN処理部との間にVPN NATを設け、グローバル側のアドレスをVPN NAT用ローカルIPアドレスとして当該保守センタから付与及び解放を行うことで実施した、特徴的構成手法、②インターネットに接続された複数のインターネットゲートウェイ端末自体及びその配下のローカルネットワークにIP接続された内線端末を、当該インターネットゲートウェイ端末とインターネットに接続されたVPNゲートウェイ間でOS I参照モデルのネットワーク層においてVPNセッションを実現するIPsecを確立することにより、当該VPNゲートウェイ配下の単一の保守サーバからリモートメンテナンスを行う実施方法であって、VPNを構築する前に、前記インターネットゲートウェイ端末からのVPN構築要求

を受けた前記保守センタが、その配下の複数のVPNゲートウェイからVPNの空きリソースのあるVPNゲートウェイを動的に選択して、当該選択されたVPNゲートウェイのグローバルIPアドレスを当該インターネットゲートウェイ端末に通知し、当該インターネットゲートウェイ端末は当該通知されたグローバルIPアドレスを当該VPNの対向ホストとして設定を行うことにより、前記リモートメンテナンスを実施する、特徴的構成手法を講じる。

【0045】本発明システムは、上記課題の解決に当たり、①各ローカルネットワークにより任意数の内線端末とIP接続してそれぞれのインターネットゲートウェイ端末の支配下とする一方、当該それぞれのインターネットゲートウェイ端末とインターネットを介してVPNゲートウェイ間でOS I参照モデルのネットワーク層においてVPNセッションを実現するIPsecを確立することで、当該VPNゲートウェイを含む単一の保守センタからリモートメンテナンスを行う実施システムであり、当該インターネットゲートウェイ端末におけるルータ部内に、その前記ローカルネットワークとVPN処理部との間にVPN NAT手段を設け、グローバル側のアドレスをVPN NAT用ローカルIPアドレスとして当該保守センタから付与及び解放を行える機能構成にシステム構築した、特徴的構成手段、②インターネットに接続された複数のインターネットゲートウェイ端末自体及びその配下のローカルネットワークにIP接続された内線端末を、当該インターネットゲートウェイ端末とインターネットに接続されたVPNゲートウェイ間でOS I参照モデルのネットワーク層においてVPNセッションを実現するIPsecを確立することにより、当該VPNゲートウェイ配下の単一の保守サーバからリモートメンテナンスを行うシステムであって、前記インターネットゲートウェイ端末からVPN構築の要求を受けると、自己の配下の複数のVPNゲートウェイからVPNの空きリソースのあるVPNゲートウェイを動的に選択して、当該選択されたVPNゲートウェイのグローバルIPアドレスを、当該要求をなしたインターネットゲートウェイ端末に通知する前記保守センタと、当該保守センタに対して前記VPN構築の要求を行うと共に、当該要求に対する当該保守センタから前記通知された前記選択されたVPNゲートウェイのグローバルIPアドレスを、当該VPNの対向ホストとして設定する前記インターネットゲートウェイ端末とを具備する、特徴的構成手段を講じる。

【0046】本発明プログラムは、上記課題の解決に当たり、①各ローカルネットワークにより任意数の内線端末とIP接続してそれぞれのインターネットゲートウェイ端末の支配下とする一方、当該それぞれのインターネットゲートウェイ端末とインターネットを介してVPNゲートウェイ間でOS I参照モデルのネットワーク層に

においてVPNセッションを実現するIPsecを確立することで、当該VPNゲートウェイを含む保守センタからリモートメンテナンスを行うシステムにて、当該インターネットゲートウェイ端末、当該保守センタにて用いられるプログラムで、グローバル側のアドレスをVPN NAT用ローカルIPアドレスとして当該保守センタから付与、解放を行う各種の処理手順を実行した、特徴的構成手順、②インターネットに接続された複数のインターネットゲートウェイ端末自体及びその配下のローカルネットワークにIP接続された内線端末を、当該インターネットゲートウェイ端末とインターネットに接続されたVPNゲートウェイ間でOS参照モデルのネットワーク層においてVPNセッションを実現するIPsecを確立することにより、当該VPNゲートウェイ配下の単一の保守サーバからリモートメンテナンスを行うシステムにて、当該インターネットゲートウェイ端末、当該保守センタにて用いられるプログラムで、当該インターネットゲートウェイ端末がVPNGWアドレス要求を行い、当該VPNGWアドレス要求に応じて当該保守サーバから通知されたVPNゲートウェイアドレスを、VPNの対向ホストとして、自己のルータ部に設定する処理手順、また、当該VPNGWアドレス要求を受信すると、自己の支配下の複数のVPNゲートウェイからVPN空きリソースのあるVPNゲートウェイを動的に選択し、そのVPNゲートウェイのグローバルIPアドレスを、当該VPNゲートウェイアドレス要求をなしたインターネットゲートウェイ端末に通知する処理手順を実行した、特徴的構成手順、を講じる。

【0047】本発明記録媒体は、上記課題の解決に当たり、本発明プログラムにより一連の完結手続を実録した、特徴的構成手続を講じる。

【0048】更に具体的に詳説すると、当該課題の解決では、本発明が次に列挙する新規な各特徴的構成手法、手段、手順又は手続を講じることにより、上記目的を達成する様になされる。

【0049】本発明方法の第1の特徴は、各ローカルネットワークにより任意数の内線端末とIP接続してそれぞれのインターネットゲートウェイ端末の支配下とする一方、当該それぞれのインターネットゲートウェイ端末とインターネットを介してVPNゲートウェイ間でOS参照モデルのネットワーク層においてVPNセッションを実現するIPsecを確立することにより、当該VPNゲートウェイを含む保守センタからリモートメンテナンスを行う実施方法であって、前記それぞれのインターネットゲートウェイ端末におけるルータ部内に、その前記ローカルネットワークとVPN処理部との間にVPN NATを設け、グローバル側のアドレスをVPN NAT用ローカルIPアドレスとして前記保守センタの保守サーバから付与及び解放を行うことにより前記リモートメンテナンスを実施してなるリモートメンテナンス実施

方法の構成採用にある。

【0050】本発明方法の第2の特徴は、上記本発明方法の第1の特徴における前記実施方法における前記リモートメンテナンスの要求が、当該要求を行う前記インターネットゲートウェイ端末が、リモートメンテナンス対象である内線端末名及び当該インターネットゲートウェイ端末のグローバルIPアドレスを、リモートメンテナンス要求コマンドとして前記保守サーバに通知すると、当該通知を受けた当該保守サーバが、当該通知したリモートメンテナンス対象の前記内線端末に付与するVPN NAT用ローカルIPアドレス及び内線端末名を、当該通知をしてきたインターネットゲートウェイ端末にリモートメンテナンス要求レスポンスとしてレスポンスすると共に、当該インターネットゲートウェイ端末のグローバルIPアドレスとの間において設置通知の際に共有されるIPsecの認証鍵を用いたIPsecによるVPNトンネルの確立を自己のVPNゲートウェイに設定させ、当該VPNゲートウェイに対してVPN NAT用ローカルIPアドレス宛のパケットを前記確立したVPNトンネルのVPN処理対象パケットとする設定を行い、前記レスポンスを受けたインターネットゲートウェイ端末が、受けた前記内線端末名に対する実ローカルIPアドレスを取得して、当該内線端末名に対する実ローカルIPアドレスと前記VPN NAT用ローカルIPアドレスとを静的NATとし自己のルータ部に対して設定を行う、以上の一連の処理を順次実施してなる、リモートメンテナンス実施方法の構成採用にある。

【0051】本発明方法の第3の特徴は、上記本発明方法の第2の特徴における前記リモートメンテナンスの実施が、前記リモートメンテナンス対象である前記内線端末に対して、前記VPN NAT用ローカルIPアドレスで前記確立されたVPNトンネルを経由して、前記保守センタから行われてなる、リモートメンテナンス実施方法の構成採用にある。

【0052】本発明方法の第4の特徴は、上記本発明方法の第2又は第3の特徴における前記リモートメンテナンスの終了が、先ず、前記VPN NAT用ローカルIPアドレスで前記確立されたVPNトンネルを経由して、当該VPNトンネルを確立させた前記インターネットゲートウェイ端末のサーバ部に対して、リモートメンテナンス終了コマンドを送信し、次に、当該送信を受けたサーバ部において、当該リモートメンテナンス終了コマンドに係る処理を行い、リモートメンテナンス終了レスポンスを送信し、その後、当該リモートメンテナンス終了レスポンスを受信した保守サーバにて、該当内線端末に対するメンテナンスが全て終了したかの第1判断を行い、当該第1判断にて肯定の場合には当該終了した内線端末は前記インターネットゲートウェイ端末の前記サーバ部、前記ルータ部の何れかであるかの第2判断を行う一方、否定の場合には判断処理を終了し、当該第2判断

にて否定の場合にはVPN NAT解放処理へ移行し、他方肯定の場合には対応する前記インターネットゲートウェイ端末に対するリモートメンテナンスを全て終了したかの第3判断を行い、当該第3判断にて肯定の場合にはVPN終了処理へ移行するとともに否定の場合には当該判断処理を終了する、以上の一連の処理を順次実施してなる、リモートメンテナンス実施方法の構成採用にある。

【0053】本発明方法の第5の特徴は、上記本発明方法の第4の特徴における前記VPN NAT解放処理が、先ず、前記保守サーバが、前記リモートメンテナンスの要求の際に設定した前記リモートメンテナンス対象の内線端末名に対するVPN NAT用ローカルIPアドレスを、前記確立したVPNトンネルへのVPN処理対象パケットから解除する一方で、前記インターネットゲートウェイ端末に対して当該リモートメンテナンス対象の内線端末名を通知した後に、当該通知を受けたインターネットゲートウェイ端末が、当該受けた内線端末名に対する実ローカルIPアドレスを取得して、それに対するVPN NAT用ローカルアドレスとの静的NATを解放し、引続き、前記保守サーバが、前記第3判断を行いその判断結果に従う、以上の一連の処理を順次実施してなる、リモートメンテナンス実施方法の構成採用にある。

【0054】本発明方法の第6の特徴は、上記本発明方法の第4又は第5の特徴における前記VPN終了処理が、前記保守サーバが、IPsecセッションの終了をVPN終了コマンドとして、前記インターネットゲートウェイ端末に通知して、当該通知を受けたインターネットゲートウェイ端末が、当該VPN終了コマンドに対する返答を当該保守サーバにVPN終了レスポンスとして送信し、前記保守サーバが、前記VPNゲートウェイに、前記リモートメンテナンスの要求に際して設定した前記VPNトンネルを解除させ、当該VPNゲートウェイと前記インターネットゲートウェイ端末間で確立されているVPNトンネル処理を終了する、以上の一連の処理を順次実施してなるリモートメンテナンス実施方法の構成採用にある。

【0055】本発明方法の第7の特徴は、上記本発明方法の第2、第3、第4、第5又は第6の特徴における前記設置通知が、新たに設置された前記インターネットゲートウェイ端末の前記サーバ部から、当該設置について前記保守サーバに設置通知コマンドを通知し、当該設置通知コマンドを受けた当該保守サーバにより、前記リモートメンテナンスのための共通情報であるIPsecの認証鍵を生成して、当該設置通知コマンドを通知してきた前記インターネットゲートウェイ端末にレスポンスし、当該レスポンスを受信した前記インターネットゲートウェイ端末は、IPsecの認証鍵を自己の前記ルータ部に対して設定する、以上の一連の処理を順次実施してなるリモートメンテナンス実施方法の構成採用にあ

る。

【0056】本発明方法の第8の特徴は、上記本発明方法の第2、第3、第4、第5、第6又は第7の特徴における前記実施方法が、前記リモートメンテナンスの要求、前記設定通知の何れか一方において、前記インターネットゲートウェイ端末の前記サーバ部及び前記ルータ部へのVPN NAT設定処理を実施してなるリモートメンテナンス実施方法の構成採用にある。

【0057】本発明方法の第9の特徴は、上記本発明方法の第2、第3、第4、第5、第6、第7又は第8の特徴における前記実施方法が、前記インターネットゲートウェイ端末に故障発生を検知した場合には、先ず、当該インターネットゲートウェイ端末が、故障通知コマンドとして故障に係る情報を前記保守サーバに送信し、次に、前記保守サーバが前記故障通知コマンドを受信すると当該故障に係る情報を処理して、当該故障通知コマンドを送信した前記インターネットゲートウェイ端末に故障通知レスポンスとして送信し、更に、当該故障通知レスポンスを受信した当該インターネットゲートウェイ端末が前記リモートメンテナンスの要求に移行する、以上の一連の処理を順次実施してなるリモートメンテナンス実施方法の構成採用にある。

【0058】本発明方法の第10の特徴は、インターネットに接続された複数のインターネットゲートウェイ端末自体及びその配下のローカルネットワークにIP接続された内線端末を、当該インターネットゲートウェイ端末と当該インターネットに接続されたVPNゲートウェイ間でOSI参照モデルのネットワーク層においてVPNセッションを実現するIPsecを確立することにより、当該VPNゲートウェイ配下の単一の保守サーバからリモートメンテナンスを行う実施方法であって、VPNを構築する前に、前記インターネットゲートウェイ端末からのVPN構築要求を受けた前記保守サーバが、その配下の複数のVPNゲートウェイからVPNの空きリソースのあるVPNゲートウェイを動的に選択して、当該選択されたVPNゲートウェイのグローバルIPアドレスを当該インターネットゲートウェイ端末に通知し、当該インターネットゲートウェイ端末は当該通知されたグローバルIPアドレスを当該VPNの対向ホストとして設定を行うことにより、前記リモートメンテナンスを実施してなるリモートメンテナンス実施方法の構成採用にある。（請求項21に対応）

【0059】本発明システムの第1の特徴は、各ローカルネットワークにより任意数の内線端末とIP接続してそれぞれのインターネットゲートウェイ端末の支配下とする一方、当該それぞれのインターネットゲートウェイ端末とインターネットを介してVPNゲートウェイ間でOSI参照モデルのネットワーク層においてVPNセッションを実現するIPsecを確立することで、当該VPNゲートウェイを含む保守センタからリモートメンテ

ナンスを行うシステムであって、前記インターネットゲートウェイ端末におけるルータ部内にそのローカルネットワークとVPN処理部との間にNATを設け、グローバル側のアドレスをVPN NAT用ローカルIPアドレスとして前記保守センタから付与及び解放を行う機能構成にシステム構築してなるリモートメンテナンス実施システムの構成採用にある。

【0060】本発明システムの第2の特徴は、上記本発明システムの第1の特徴における前記保守センタが、前記インターネットゲートウェイ端末からリモートメンテナンス対象の内線端末名の通知を受けて当該リモートメンテナンス対象の内線端末名に対応するVPNアクセス用のVPN NAT用ローカルアドレスの付与を行う保守サーバと、前記リモートメンテナンスを行うリモートメンテナンス装置と、当該リモートメンテナンス装置からの、当該リモートメンテナンス対象の内線端末名に対応するVPN NAT用ローカルIPアドレスへアクセスを經由するVPNゲートウェイとを、保守センタローカルネットワークにてネットワーク構築してなるリモートメンテナンス実施システムの構成採用にある。

【0061】本発明システムの第3の特徴は、上記本発明システムの第1又は第2の特徴における前記インターネットゲートウェイ端末が、前記保守センタにリモートメンテナンス対象の内線端末名を通知するサーバ部と、当該通知したことにより当該保守センタから付与されたVPNアクセス用のVPN NAT用ローカルIPアドレスと当該リモートメンテナンス対象の内線端末名のIPアドレスを割りつけるVPN NAT及び当該保守センタの前記VPNゲートウェイとVPNトンネルを確立するVPN処理部のルータ部とで構成して、前記VPNゲートウェイを介した、リモートメンテナンス対象端末名に対するVPN NAT用ローカルIPアドレスへのアクセスにより、前記リモートメンテナンスを行うリモートメンテナンス装置からの、前記内線端末へのパケット転送を可能ならしめる機能を構築してなるリモートメンテナンス実施システムの構成採用にある。

【0062】本発明システムの第4の特徴は、インターネットに接続された複数のインターネットゲートウェイ端末自体及びその配下のローカルネットワークにIP接続された内線端末を、当該インターネットゲートウェイ端末と当該インターネットに接続されたVPNゲートウェイ間でOSI参照モデルのネットワーク層においてVPNセッションを実現するIPsecを確立することにより、当該VPNゲートウェイ配下の単一の保守サーバからリモートメンテナンスを行うシステムであって、前記インターネットゲートウェイ端末からVPN構築の要求を受けると、その配下の複数のVPNゲートウェイからVPNの空きリソースのあるVPNゲートウェイを動的に選択して、当該選択されたVPNゲートウェイのグローバルIPアドレスを、当該要求をなしたインターネ

ットゲートウェイ端末に通知する前記保守センタと、当該保守センタに対して前記VPN構築の要求を行うと共に、当該要求に対する当該保守センタから前記通知された前記選択されたVPNゲートウェイのグローバルIPアドレスを、当該VPNの対向ホストとして設定する前記インターネットゲートウェイ端末とを具備してなるリモートメンテナンス実施システムの構成採用にある。

(請求項22に対応)

【0063】本発明プログラムの第1の特徴は、各ローカルネットワークにより任意数の内線端末とIP接続してそれぞれのインターネットゲートウェイ端末の支配下とする一方、当該それぞれのインターネットゲートウェイ端末とインターネットを介してVPNゲートウェイ間でOSI参照モデルのネットワーク層においてVPNセッションを実現するIPsecを確立することで、当該VPNゲートウェイを含む保守センタからリモートメンテナンスを行うシステムにおける、当該インターネットゲートウェイ端末で用いられるプログラムであって、当該インターネットゲートウェイ端末が設置された後に、リモートメンテナンスサービスを利用する場合に、前記保守センタに対して設置した旨を通知する設置通知処理を当該インターネットゲートウェイ端末に行わせる前記プログラムの実行により、前記設置について前記保守センタの保守サーバに設置通知コマンドを通知した後に、当該保守サーバからの当該設置通知コマンドに対するレスポンスを受信すると当該レスポンスとして受けたIPsecの認証鍵を自己のルータ部に対して設定する、一連の手順を踏んでなるリモートメンテナンス実施プログラムの構成採用にある。

【0064】本発明プログラムの第2の特徴は、各ローカルネットワークにより任意数の内線端末とIP接続してそれぞれのインターネットゲートウェイ端末の支配下とする一方、当該それぞれのインターネットゲートウェイ端末とインターネットを介してVPNゲートウェイ間でOSI参照モデルのネットワーク層においてVPNセッションを実現するIPsecを確立することで、当該VPNゲートウェイを含む保守センタからリモートメンテナンスを行うシステムにおける、当該インターネットゲートウェイ端末にて用いられるプログラムであって、当該インターネットゲートウェイ端末への、前記内部端末からのWEBアクセス、当該インターネットゲートウェイ端末の操作者によるボタン操作の何れかにより、リモートメンテナンスを要求するリモートメンテナンス要求処理を当該インターネットゲートウェイ端末に行わせる前記プログラムの実行により、リモートメンテナンス対象である前記内線端末名及び前記インターネットゲートウェイ端末のグローバルIPアドレスを、リモートメンテナンス要求コマンドとして前記保守サーバに通知した後に、前記リモートメンテナンス要求コマンドに対するレスポンスを受けて、当該レスポンスとして受けた、

内線端末名に対する実ローカルIPアドレスを取得して、当該内線端末名に対する実ローカルIPアドレスと当該レスポンスとして受けたVPN NAT用ローカルIPアドレスとを静的NATとして設定させる、以上の一連の手順を踏んでなるリモートメンテナンス実施プログラムの構成採用にある。

【0065】本発明プログラムの第3の特徴は、各ローカルネットワークにより任意数の内線端末とIP接続してそれぞれのインターネットゲートウェイ端末の支配下とする一方、当該それぞれのインターネットゲートウェイ端末とインターネットを介してVPNゲートウェイ間でOS I参照モデルのネットワーク層においてVPNセッションを実現するIPsecを確立することで、当該VPNゲートウェイを含む保守センタからリモートメンテナンスを行うシステムにおける、当該インターネットゲートウェイ端末にて用いられるプログラムであって、前記保守センタより行われる前記リモートメンテナンスの作業が終了した旨の通知に係るリモートメンテナンス終了処理を、当該通知を受けた前記インフェースゲートウェイ端末に行わせる前記プログラムの実行により、前記保守センタからのリモートメンテナンス終了コマンドの受信を契機に、当該リモートメンテナンス終了コマンドに関する処理を行い、リモートメンテナンス終了レスポンスを送信して、前記保守センタからVPN解放コマンドとしてリモートメンテナンス対象の内線端末名の通知を受けた場合には、当該受けた内線端末名に対する実ローカルIPアドレスを取得し、取得した実ローカルIPアドレスに対するVPN NAT用ローカルアドレスとの静的NATを解放する、以上の一連の手順を踏んでなるリモートメンテナンス実施プログラムの構成採用にある。

【0066】本発明プログラムの第4の特徴は、各ローカルネットワークにより任意数の内線端末とIP接続してそれぞれのインターネットゲートウェイ端末の支配下とする一方、当該それぞれのインターネットゲートウェイ端末とインターネットを介してVPNゲートウェイ間でOS I参照モデルのネットワーク層においてVPNセッションを実現するIPsecを確立することで、当該VPNゲートウェイを含む保守センタからリモートメンテナンスを行うシステムにおいて、当該保守センタにて用いられるプログラムであって、前記リモートメンテナンスの要求に対応するリモートメンテナンス要求処理を前記保守サーバに行わせる前記プログラムの実行により、前記要求を受けて、前記リモートメンテナンスの要求に係るリモートメンテナンス対象の前記内線端末に付与するVPN NAT用ローカルIPアドレス及び内線端末名を、当該要求を行った前記インターネットゲートウェイ端末にリモートメンテナンス要求レスポンスとして送信すると共に、当該インターネットゲートウェイ端末のグローバルIPアドレスとの間において共有されるI

Psecの認証鍵を用いたIPsecによるVPNトンネルの確立を、自己のVPNゲートウェイに指示し、自己の当該VPNゲートウェイに対して、VPN NAT用ローカルIPアドレス宛のパケットを、当該指示により確立されるVPNトンネルのVPN処理対象パケットとする設定を行う、以上の一連の手順を踏んでなるリモートメンテナンス実施プログラムの構成採用にある。

【0067】本発明プログラムの第5の特徴は、各ローカルネットワークにより任意数の内線端末とIP接続してそれぞれのインターネットゲートウェイ端末の支配下とする一方、当該それぞれのインターネットゲートウェイ端末とインターネットを介してVPNゲートウェイ間でOS I参照モデルのネットワーク層においてVPNセッションを実現するIPsecを確立することで、当該VPNゲートウェイを含む保守センタからリモートメンテナンスを行うシステムにて、当該保守センタにて用いられるプログラムであって、新たに設置された前記インターネットゲートウェイ端末からの設置通知コマンドを処理する設定通知コマンド処理を前記保守センタに行わせる前記プログラムの実行により、前記設置通知コマンドに応じて、前記リモートメンテナンスのための共通情報であるIPsecの認証鍵を生成して、当該設置通知コマンドを通知してきた前記インターネットゲートウェイ端末にレスポンスする、以上の一連の手順を踏んでなるリモートメンテナンス実施プログラムの構成採用にある。

【0068】本発明プログラムの第6の特徴は、各ローカルネットワークにより任意数の内線端末とIP接続してそれぞれのインターネットゲートウェイ端末の支配下とする一方、当該それぞれのインターネットゲートウェイ端末とインターネットを介してVPNゲートウェイ間でOS I参照モデルのネットワーク層においてVPNセッションを実現するIPsecを確立することで、当該VPNゲートウェイを含む単一の保守センタからリモートメンテナンスを行うシステムにおいて、当該保守センタにて用いられるプログラムであって、前記保守センタにおける終了ボタンが押されたことを契機に、前記リモートメンテナンスの作業が終了したことを通知するリモートメンテナンス終了処理を、前記保守サーバに行わせる前記プログラムの実行により、VPN NAT用ローカルIPアドレスで確立されたVPNトンネルを経由して、当該VPNトンネルを確立させた前記インターネットゲートウェイ端末のサーバ部に対して、リモートメンテナンス終了コマンドを送信した後に、当該リモートメンテナンス終了のレスポンスを受信すると、該当内線端末に対するメンテナンスが全て終了したかの第1判断を行い、当該第1判断にて肯定の場合には当該終了した前記内線端末は前記インターネットゲートウェイ端末の前記サーバ部かルータ部かの何れかであるかの第2判断を行う一方、否定の場合にはこのプログラムを終了し、

当該第2判断にて否定の場合にはVPN NAT解放処理へ移行する一方、肯定の場合には対応する前記インターネットゲートウェイ端末に対するリモートメンテナンスを全て終了したかの第3判断を行い、当該第3判断にて肯定の場合にはVPN終了処理へ移行する一方、否定の場合にはこのプログラムを終了する、以上の一連の手順を踏んでなるリモートメンテナンス実施プログラムの構成採用にある。

【0069】本発明プログラムの第7の特徴は、上記本発明プログラムの第6の特徴における前記VPN NAT解放処理が、リモートメンテナンス要求を受けて設定したリモートメンテナンス対象の内線端末名に対するVPN NAT用ローカルIPアドレスを、確立した前記VPNトンネルへのVPN処理対象パケットから解除する様、前記VPNゲートウェイに対して行い、前記インターネットゲートウェイ端末に対して、リモートメンテナンス対象の内線端末名を通知し、その後、前記第3判断にリターンする一連の処理であり、前記VPN終了処理が、IPsecセッションの終了をVPN終了コマンドとして、前記インターネットゲートウェイ端末に対して送信して、前記VPNゲートウェイに、リモートメンテナンス実施要求の際に設定した前記VPNトンネルの解除させ、当該VPNゲートウェイと当該インターネットゲートウェイ端末間で確立されているVPNトンネル処理を終了させる一連の処理であるリモートメンテナンス実施プログラムの構成採用にある。

【0070】本発明プログラムの第8の特徴は、インターネットに接続された複数のインターネットゲートウェイ端末自体及びその配下のローカルネットワークにIP接続された内線端末を、当該インターネットゲートウェイ端末と当該インターネットに接続されたVPNゲートウェイ間でOSI参照モデルのネットワーク層においてVPNセッションを実現するIPsecを確立することにより、当該VPNゲートウェイ配下の単一の保守サーバからリモートメンテナンスを行うシステムにおける、当該インターネットゲートウェイ端末にて用いられるプログラムであって、前記内線端末からのリモートメンテナンス要求の登録又はインターネットゲートウェイ端末管理者による前記インターネットゲートウェイ端末本体のボタン操作の何れかにより、VPNゲートウェイアドレスを要求するVPNゲートウェイアドレス要求処理を当該インターネットゲートウェイ端末に行わせる前記プログラムの実行により、前記保守センタに対して前記VPNゲートウェイアドレスの要求を行うと共に、当該保守センタから当該要求に対するVPNゲートウェイアドレス要求レスポンスを受信すると、当該VPNゲートウェイアドレス要求レスポンスとして受信したVPNゲートウェイグローバルIPアドレスを、VPNの対向ホストとして、自己のルータ部に設定して、前記リモートメンテナンス要求の処理を行う、以上の一連の手順を踏んでなるリモートメンテナンス実施プログラムの構成採用にある。

でなるリモートメンテナンス実施プログラムの構成採用にある。(請求項23に対応)

【0071】本発明プログラムの第9の特徴は、インターネットに接続された複数のインターネットゲートウェイ端末自体及びその配下のローカルネットワークにIP接続された内線端末を、当該インターネットゲートウェイ端末とインターネットに接続されたVPNゲートウェイ間でOSI参照モデルのネットワーク層においてVPNセッションを実現するIPsecを確立することにより、当該VPNゲートウェイ配下の単一の保守サーバからリモートメンテナンスを行うシステムにおける、当該保守センタにて用いられるプログラムであって、前記インターネットゲートウェイ端末からのVPNゲートウェイアドレス要求に伴う前記保守センタ内の処理であるVPNゲートウェイアドレス要求処理を当該保守センタに行わせる前記プログラムの実行により、前記インターネットゲートウェイ端末から前記VPNゲートウェイアドレス要求を受信すると、自己の支配下の複数のVPNゲートウェイからVPN空きリソースのあるVPNゲートウェイを動的に選択し、そのVPNゲートウェイのグローバルIPアドレスを、当該VPNゲートウェイアドレス要求をなしたインターネットゲートウェイ端末に通知する、以上の一連の手順を踏んでなるリモートメンテナンス実施プログラムの構成採用にある。(請求項24に対応)

【0072】本発明記録媒体の第1の特徴は、上記本発明プログラムの第1、第2、第3、第4、第5、第6又は第7の特徴における前記プログラムによる一連の手続を実録してなるリモートメンテナンス実施プログラムを記録した記録媒体の構成採用にある。

【0073】本発明記録媒体の第2の特徴は、上記本発明プログラムの第7又は第9の特徴における前記プログラムによる一連の手続を実録してなるリモートメンテナンス実施プログラムを記録した記録媒体の構成採用にある。(請求項25に対応)

【0074】

【発明の実施の形態】以下、添付図面を参照して、本発明の実施の形態をそのシステム例、方法例、記録媒体例及びプログラム例について詳細を説明する。

【0075】(システム例)図1に本発明の一実施形態であるリモートメンテナンス実施システム例の構成図を示す。リモートメンテナンスシステムは、インターネットゲートウェイ端末1(以下、情流GW端末)、内線端末2a~2n(nは任意の自然数を表す)、保守サーバ3、リモートメンテナンス装置4、VPNゲートウェイ5(5a~5n)の5つのノードからシステム構築される。

【0076】前記情流GW端末1は、通常インターネット6(WAN)側とローカルネットワークである内線(LAN)7側のいずれともTCP/IPで通信するこ

とを前提とする。また、保守サーバ3側のLAN8上のVPNゲートウェイ5(5a~5n)とVPNを構築できる機能を持つことが必要がある。

【0077】従来のルータfやアプリケーションゲートウェイと呼ばれる物が対象となる。従来のISDNターミナルアダプタのように、それ自体ではTCP/IPの通信を行わない物は対象としない。以下の記述において、単に「端末」の呼称は、情流GW端末1を指す。

【0078】前記内線端末2a~2nは、前記情流GW端末1配下の内線LAN7に接続するPC(パソコン)等の端末(群)である。内線LAN7に接続されている情流GW端末1本体に含まれるサーバ部10やルータ部11も内線端末2a~2nとして扱う。前記保守センタ9は、保守サーバ3、リモートメンテナンス装置4、VPNゲートウェイ5(5a~5n)を構成要素とするリモート保守を行うセンタの総称である。

【0079】前記保守サーバ3は、情流GW端末1や内線端末2a~2nのリモートメンテナンスに関する情報を管理するインターネット6上のサーバで、インターネット6側とリモートメンテナンス装置4が存在するLAN8側に各々LANインターフェースを持つ。

【0080】前記リモートメンテナンス装置4は、情流GW端末1や内線端末2a~2nのリモートメンテナンスを行うオペレーティング装置で、WEBブラウザ機能を持つことが前提である。前記VPNゲートウェイ5a~5nは、インターネット6経由で、情流GW端末1と保守センタ9を結ぶVPNを構築するためのVPNゲートウェイ装置である。

【0081】前記情流GW端末1は、httpサーバ処理を行うhttpサーバ部100と、httpサーバから呼ばれて内部処理を行うCGI処理部101と、ルータ部11への制御コマンドを発行するルータ設定処理部102と、保守サーバ3にコマンドを送信するコマンド送出処理部103を含むサーバ部10と、IPsecを含んだIPルータ処理を制御するルータ部11から構成される。

【0082】前記保守サーバ3は、端末1からのhttpコマンドを受信するhttpサーバ部30と、httpサーバ部30から呼ばれて内部処理を行うCGI処理部31と、VPNゲートウェイ1へtelnetコマンドを発行するVPNゲートウェイ設定処理部32から構成される。前記VPNゲートウェイ5a~5nは、端末1のルータ部11とVPNセッションを行うVPN処理部50と、保守サーバ3からのtelnetコマンドを受信する設定コマンド受信処理部51から構成される。

【0083】前記リモートメンテナンス装置4は、端末1のサーバ部10へhttpプロトコル等でコマンドを送出するメンテナンスコマンド処理部40から構成される。以上、示した、保守サーバ3と、VPNゲートウェイ5a~5nと、リモートメンテナンス装置4を使っ

て、保守センタ9からインターネット6のVPNトンネル12経由で、複数の情流GW端末1及びその内線端末2a~2nをリモートメンテナンスする際、情流GW端末1配下のローカルネットワークアドレスが如何なる場合でも、同時にVPNリモートメンテナンスを実現する。

【0084】(方法例)前記システム例に適用する本方法例におけるVPNリモートメンテナンスは、設置通知処理と、VPNGWアドレス要求と、リモートメンテナンス要求処理と、リモートメンテナンス終了処理と、VPN NAT解放処理と、VPN終了処理と、故障通知処理との7つの「通知コマンド及びレスポンス」と、実際に保守センタ9のオペレータが行う「リモートメンテナンス実施」(本リモートメンテナンスプロトコルにおいては、実際のメンテナンス作業のプロトコルについては、特に規定しない。それは、TCP/IPを利用していれば、汎用のアプリケーションであってもよいし、独自のプロトコルでもよい。)を通信プロトコルとして構成される。

【0085】ここで、リモートメンテナンス実施以外の7つの通信プロトコルは実際のメンテナンス作業(以下、リモートメンテナンス実施)を行うための、手法にすぎず、あくまでも主旨は、以下の通りである。

【0086】すなわち、第一の主旨は、リモートメンテナンス装置4からメンテナンス対象内線端末2a~2nに対して、VPNのトンネル12を利用してTCP/IPプロトコルを利用するアプリケーションで行い、このとき、保守センタ9のリモートメンテナンス装置4から、メンテナンス対象内線端末2a~2nへのIP接続をVPN NAT用ローカルIPアドレスを用いて、ルータ部11内に機能構成する後記VPN NAT110で行うことにより、先に述べた複数の情流GW端末1へのアクセスをその配下のIPアドレスが重複している場合でも確実に実施することにある。ただし、当該NATを経由すると実施不可能なアプリケーションは実施できないのは、制限事項である。

【0087】また、第二の主旨は、リモートメンテナンス装置4からメンテナンス対象内線端末2a~2nに対して、VPNのトンネル12を利用してTCP/IPプロトコルを利用するアプリケーションで行い、このとき、保守センタ9のVPNゲートウェイ5a~5nが増設などによりアドレスが変更された場合でも、リモートメンテナンス装置4から任意のVPNゲートウェイ5a~5n及びインターネットゲートウェイを介して、メンテナンス対象内線端末へのIP接続が確実に実行されることにある。

【0088】以下、前記第一の主旨を達成するための、本方法例を以下図面を参照して説明する。当該本方法例はルータ部11内に機能構成するVPN NAT110に動的にVPN NAT用ローカルIPアドレスを付与する

ことにある。図2をもとにVPNNAT110に動的にVPNNAT用ローカルIPアドレスを付与する機能の概略を説明する。

【0089】まず、①で保守センタ9にリモートメンテナンス対象端末の内線端末2a～2n名を通知する。②で、保守センタ9は、情流GW端末1に対して、情流GW端末1のサーバ部10経由でリモートメンテナンス対象内線端末2a～2n名に対応するVPNアクセス用のVPNNAT用ローカルIPアドレス(10.0.0.1)を付与する。これは、基本的にリモートメンテナンス要求の時点で行われる。

【0090】次に③で、VPNNAT用ローカルIPアドレスとリモートメンテナンス対象内線端末2a～2nのIPアドレスを静的NAT110で割り付ける。これも、②に引き続きリモートメンテナンス要求時に行われる。次に④でリモートメンテナンス実施時にVPNトンネル12の中を通してVPNNAT用ローカルIPアドレスへアクセスする。そうすると、⑤に示すように、リモートメンテナンス対象内線端末2a～2nへパケットが転送されアクセス可能になる。

【0091】このように事前に静的にVPNNAT用ローカルIPアドレスを割り付けなくても動的にVPNNAT用ローカルIPアドレスを付与することにより、複数の情流GW端末1へのアクセスをその配下のIPアドレスが重複している場合でも同時に実施とすることができるようになる。

【0092】以下、第2の主旨を達成する方法例として、VPN構築に先立ち、保守センタ9がその配下の複数のVPNゲートウェイ5a～5nからVPNの空のリソースのあるVPNゲートウェイ5iを動的に選択し、情流GW端末のルータ部11に通知することにより、ルータ部11内に設置されるVPNゲートウェイのグローバルIPアドレスを動的にVPNの対向ホストとして設定付与することにある。

【0093】以下、本方法例を実現するための6つのプロトコルについて概要を説明する。前記設置通知処理は、情流GW端末1が設置されたことを保守サーバ3に通知し、保守サーバ3からリモートメンテナンスのための共有情報(IPsecのPreshared Key、端末認証パスワード(以下、Secret(ID2))等)を暗号化して受け取ることが主旨である。

【0094】また、前記主旨を実現するために、設置通知処理内でも、情流GW端末1のサーバ部10とルータ部11に対してVPNNAT110を構築するのも本方法例においては大きな目的である。

【0095】前記VPNGWアドレス要求処理は、保守サーバ3が保守センタ9配下の複数のVPNゲートウェイ5a～5nからVPNの空のリソースのあるVPNゲートウェイ5iを動的に選択して、そのVPNゲートウェイ5iのグローバルIPアドレスをVPNゲートウ

ェイ通知レスポンスとして情流GW端末1に通知し、情流GW端末ルータ部11は通知されたVPNゲートウェイ5iのグローバルIPアドレスをVPNの対向ホストとして設定を行うことも本方法においては大きな主旨である。

【0096】前記リモートメンテナンス要求処理は、IPsecによるリモートメンテナンスの実施を保守サーバ3に要求することを主旨とする。リモートメンテナンス要求処理に対応するメンテナンス対象端末は、情流GW端末1本体、及び、内線端末2a～2nとする。また、主旨を実現するために、リモートメンテナンス要求処理内でも、情流GW端末1のサーバ部10とルータ部11以外の内線端末2a～2nに対してVPNNAT110を構築するのも本方法例においては大きな主旨である。

【0097】前記リモートメンテナンス終了処理は、リモートメンテナンス装置4を使って実際にリモートメンテナンスが終了したことを対象となる情流GW端末1に伝えることを主旨とする。

【0098】前記VPNNAT110解放処理は、リモートメンテナンスが終了した情流GW端末1のサーバ部10とルータ部11以外の内線端末2a～2nについてVPNNAT110を解放することを目的とする。これにより、後の効果に述べるように、VPNNAT用ローカルIPアドレス資源を有効活用可能となる。VPN終了処理は、IPsecセッションを終了することを主旨とする。

【0099】(プログラム例、記録媒体例)本方法例を実施するためのプログラム例及び記録媒体例を図面につき説明する。リモートメンテナンスの全体処理フロー図3～図9を用いて、各通信データの流れを示す。各図の“→”は、設置通知処理、VPNGWアドレス要求処理、リモートメンテナンス要求処理、リモートメンテナンス終了処理、VPNNAT解放処理、VPN終了処理、故障通知処理の際の通信シーケンスにおけるコマンド送出及び受信を示した手順及び手続の流れである。

【0100】処理形態は、情流GW端末1設置時に一度だけ、情流GW端末1設置者の操作を契機として、図3に示す設置通知処理の①設置通知コマンド(端末ID、公開鍵、原文、MAC)→②設置通知レスポンス(暗号化Preshared Key、暗号化Secret ID2、暗号化保守者パスワード、暗号化サーバ部用VPNNAT用ローカルIPアドレス、暗号化ルータ部用VPNNAT用ローカルIPアドレス、暗号化ルータ部用VPNNAT用ローカルIPアドレス)→③ルータ設定(VPNNAT110、暗号化Preshared Key)が行われる。

【0101】その後、内線端末2a～2nユーザ(以下、ユーザ)が情流GW端末1から保守センタ9(以下、センタ)に対して、内線端末2a～2nのリモートメンテナンスの要求をすれば、思い立った度毎に、内線端

末ユーザの操作を契機として、図4に示すVPNGWアドレス要求の①VPNGWアドレス要求コマンド（端末ID、公開鍵、原文、MAC）→②VPNGW選択処理→③VPNGWアドレス要求レスポンス（VPNゲートウェイグローバルIPアドレス）→④ルータ設定（VPNゲートウェイグローバルIPアドレス）が行われる。

【0102】次に、VPNGWアドレス要求の処理終了を契機として、図5に示すリモートメンテナンス要求の①リモートメンテナンス要求コマンド（端末ID、内線端末2a～2n名、情流GW端末グローバルアドレス、要求者レベル、緊急度、要求者名、電話番号、要求内容）→②VPNNAT用ローカルIPアドレス割り当て処理→③VPNNAT用ローカルIPアドレス向けルーティング設定→④IPsec設定処理→⑤リモートメンテナンス要求レスポンス（内線端末2a～2n名、VPNNAT用ローカルIPアドレス、受付番号）→⑥VPNNAT用ローカルIPアドレスのVPNNAT110設定が行われる。

【0103】センタ9では、オペレータがリモートメンテナンス装置4からリモートメンテナンス要求の受信を随時確認している。オペレータが、各々のリモートメンテナンス要求処理に対するリモートメンテナンスを実施すると思いついた度毎に、オペレータの操作により、図6に示す①リモートメンテナンス実施が行われる。

【0104】センタ9では、各々のリモートメンテナンス要求処理に対するリモートメンテナンスが終了した度毎に、オペレータの操作により、図7に示すリモートメンテナンス終了処理の①リモートメンテナンス終了コマンド（受付番号）→②リモートメンテナンス終了レスポンスが行われる。

【0105】リモートメンテナンス終了処理後、保守サーバ3の判断により、必要に応じて、自動的に、図8に示すVPNNAT解放処理の①VPNNAT110解放コマンド（内線端末2a～2n名）→②VPNNAT用ローカルIPアドレスVPNNAT設定解除→③VPNNAT110解放レスポンス→④VPNNAT用ローカルIPアドレス変換処理→⑤VPNNAT用ローカルIPアドレスルーティング設定解除が行われる。

【0106】VPNNAT110解放終了後、保守サーバ3の判断により、必要に応じて、自動的に図9に示すVPN終了の①VPN終了コマンド→②VPNNAT用ローカルIPアドレス初期化設定→③VPN終了レスポンス→④VPNNAT用ローカルIPアドレス向けルーティング初期化→⑤IPsec設定解除が行われる。

【0107】以上が、全体フローの概略である。なお、情流GW端末1台に着目した場合の情流GW端末1及び保守センタ9の処理フローを図10、図11のフローチャートに示す。

【0108】即ち、図10に示す情流GW端末1側フローチャートについては、設置通知STcはSTa→ST

bを順次踏んで実践され、リモートメンテナンス終了処理SThは設置通知STcからSTd→STeを踏んで、VPNNAT解放処理STiは設置通知STcからSTd→STe→STfを踏んで、VPN終了処理STjは設置通知STcからSTd→STe→STf→STgを踏んで、故障通知STnは設置通知STcからSTd→STk→STlを踏んで、VPNGWアドレス要求SToは設置通知STcからSTd→STkを踏むが故障通知STnから直結して踏んで、リモートメンテナンス要求STmは設置通知STcからSTd→STk→SToを踏むがSTd→STk→STl→STn→SToを踏んで、それぞれ実践され、その間必要に応じて繰り返しが入る。

【0109】図11に示すセンタ9側フローチャート（情流GWID=N）については、設置通知処理ST6はST1→ST2→ST3を、VPNGWアドレス要求処理ST16はST1→ST2→ST3→ST15を、リモートメンテナンス要求処理ST7はST1→ST2→ST3→ST15→ST4を、故障通知処理ST8はST1→ST2→ST3→ST15→ST4→ST5を、それぞれ順次踏んで実践される。

【0110】リモートメンテナンス終了ST9はST1→ST2を踏んで、VPNNAT解放ST12はリモートメンテナンス終了ST9からST10→ST11を踏んで、VPN終了ST14はVPNNAT解放ST12からST13を踏んで、それぞれ実践され、その間必要に応じて繰り返しが入る。なお、図26に示す故障通知は、故障発生時に通知されるが、全体の流れとは独立な処理なのでここでは詳細にはふれない。

【0111】「リモートメンテナンス実施のための前提条件」なお、本実施形態例を実行するためには、以下の前提条件が必要である。

（1）保守サーバ3と端末1では、共有秘密情報（以下、Secret（ID））を事前に共有していること。Secret（ID）は、出荷時に端末1にROM等に埋め込み、保守サーバ3と共有することで対応する。なおSecret（ID）は、保守サーバ3がリモートメンテを行うすべての端末1に共通とする。

【0112】（2）端末1のルータ部11は、IPsec等のIPレベルのVPN機能を持つこと。また、VPNセッションについて、セッション待ち受け側の設定を事前に行っておくこと（IPsecの場合は、レスポンスとして設定しておくこと）。また、Preshared keyはダミーデータを設定しておくこと。

（3）保守センタ9のVPNゲートウェイ5は、VPNセッションについて、セッション確立側の設定を事前に行っておくこと（IPsecの場合は、イニシエータとして設定しておくこと）。

【0113】（4）VPNゲートウェイ5は、端末1のルータ部11と通信互換性のあるVPN機能を持つこ

と。

(5) 端末 1 のルータ部 11 は、保守サーバ 3 の公開されたグローバル IP アドレス (または、インターネットホスト名) を設置通知の時点までに事前に知っていること。また、インターネット 6 へ接続設定が完了していること。

【 0114 】 (6) ルータ設定処理部 102 からルータ部 11 への各種設定はリモートコンソール (以下、`telnet`)、またはプロセス間通信 (ソケット通信等) で行えること。

(7) 保守サーバ 3 の VPN ゲートウェイ設定処理部 32 から VPN ゲートウェイ 5 の設定コマンド受信処理部 51 への各種設定は `telnet` またはプロセス間通信 (ソケット通信等) で行えること。

【 0115 】 (8) 保守サーバ 3 上には、VPN NAT 110 DB を持つ。テーブルは、VPN NAT 用ローカル IP アドレスをキーとした複数レコードから構成され、フィールドとして、割り当て情流 GW 端末 ID / 端末名を持つ。

(9) 情流 GW 端末 1 には、ホストテーブルを持つ。テーブルは、内線端末 2 a ~ 2 n 名をキーとした複数レコードから構成され、フィールドとして、実 IP アドレス、VPN NAT 用ローカル IP アドレスを持つ。初期状態では、ホストテーブルは空である。

【 0116 】 (10) 保守サーバ 3 上の VPNGW 5 (5 a ~ 5 n) は複数の存在を可能とする。一つの VPNGW 5 はその VPNGW 5 が許容する複数個の VPN トンネル 12 を構成可能とする。

(11) 保守サーバ 3 上には VPNGW トンネルテーブルを持つ。テーブルは、VPN ゲートウェイ 5 の IP アドレス及び VPN トンネル番号をキーとした複数のレコードから構成され、フィールドの値として、割り当て情流 GW ID を持つ。

【 0117 】 [処理シーケンスの説明] 以下、図 3 ~ 図 9 と、図 12 ~ 図 25 を用いて、各処理の手順について詳細を説明する。書中左に振っている番号 $n - n$ (n は任意の自然数) は、図中のステップ処理番号に対応する。

【 0118 】 < 設置通知処理 > 図 3、図 12 及び図 13 に示すよう設置通知は、端末 1 が設置されたことを保守サーバ 3 に通知し、保守サーバ 3 からリモートメンテナンスのための共有情報 (IPsec の Preshared Key、端末 1 認証パスワード (以下、Secret (ID2))、保守者パスワード) を暗号化して受け取り、それを設定することが目的である。

【 0119 】 設置通知処理以降の端末認証処理に Secret (ID) の代わりに、Secret (ID2) を使うのは、端末 1 全てに共通である Secret (ID) よりも、Secret (ID2) を使った方がセキュリティが強化されるためである。また、VPN を構築する際、各情流 GW 端末 1 配下のプ

ライベート IP アドレスの重複が考えられるため、それを避けるために、VPN NAT 処理を行う。そのための、VPN 用ダミープライベート IP アドレス (以下、VPN NAT 用ローカル IP アドレス) を保守サーバ 3 から受け取ることが第 2 の目的である。

【 0120 】 ① 設置通知コマンド (端末サーバ部 10 → 保守センタ 9)

((通信契機))

1-1 端末 1 設置終了後、ルータ部 11 がインターネット 6 への接続設定が完了した時点で、サーバ部 10 に対するボタン操作により行う。設置通知は一度だけ行えばよい。

【 0121 】 ((端末前処理))

1-2 サーバ部 10 のコマンド送出処理部 103 は、秘密鍵と公開鍵を生成する。アルゴリズムには RSA 等の公開鍵暗号を使用する。

1-3 「端末 1 のユニークな ID + タイムスタンプ」から認証のための原文を作成する。

1-4 原文に対して、Secret (ID) を用いたメッセージ認証子 (MAC) を生成する (ISO9797-1、ISO9797-2 に準拠することが望ましい)。

【 0122 】 ((コマンド送信処理))

1-5 端末 ID、公開鍵、原文、MAC をパラメータとして、端末 1 (サーバ部 10 / コマンド送出処理部 103) から保守サーバ 3 (http サーバ部 30) への http コマンドで < 非 IPsec セッション > として設置通知コマンドを送信する。

【 0123 】 ② 設置通知レスポンス (保守サーバ 3 → 端末サーバ部 10)

((保守サーバ処理))

1-6 保守サーバ 3 の http サーバ部 30 は、受信したコマンド名とパラメータを CGI 処理部 31 に渡し、CGI 処理部 31 は、原文に対して、Secret (ID) を用いたメッセージ認証子 (MAC) を生成して (端末 1 と同様の演算)、受信した MAC と一致することを確認する (端末認証)。

【 0124 】 1-7 CGI 処理部 31 は、IPsec の認証鍵 (Preshared Key)、Secret (ID2) をランダムに生成し、保守者パスワードを設定ファイルから取得し、端末 1 DB 中の端末 ID に対応するレコードを新規にクリエイトし (既に存在する場合は上書き)、該当レコードの各フィールドに保持する。

【 0125 】 1-8 CGI 処理部 31 は、VPN NAT DB 91 から空き VPN NAT 用ローカル IP アドレスをサーバ部 10 用とルータ部 11 用に二つ選択し、該当レコードの割り当て状況フィールドに情流 GW 端末 ID / 端末名を保持するとともに、端末 1 DB のサーバ部 10 VPN NAT 用ローカル IP アドレス及びルータ部 11 VPN NAT 用ローカル IP アドレスフィールドに VPN NAT 用ローカル IP アドレスを保持する。

【0126】1-9 CGI処理部31は、IPsecの認証鍵(Preshared Key)、Secret (ID2)、保守者パスワード、サーバ部10及びルータ部11用VPN NAT用ローカルIPアドレスを、情流GW端末1の公開鍵で暗号化する。

【0127】((レスポンス送信処理))

1-10 保守サーバ3のhttpサーバ部30は、ステータス(正常またはエラーステータス(認証異常等))、端末1の公開鍵で暗号化したIPsecの認証鍵(Preshared Key)、端末1の公開鍵で暗号化したSecret (ID2)、端末1の公開鍵で暗号化した保守者パスワード、端末1の公開鍵で暗号化したサーバ部用VPN NAT用ローカルIPアドレス、端末1の公開鍵で暗号化したルータ部用VPN NAT用ローカルIPアドレスをパラメータとしたデータをCGI処理部31から受けて、保守サーバ3(httpサーバ部30)から端末1(サーバ部10/コマンド送出処理部103)へのhttpレスポンス<非IPsecセッション>としてレスポンスを送信する。

【0128】③サーバ部10とルータ部11のVPN NAT110設定(端末サーバ部10→端末ルータ部11)

((端末後処理))

1-11 端末サーバ部10は、端末1の秘密鍵で、IPsecの認証鍵(Preshared Key)、Secret (ID2)、保守者用パスワード、サーバ部用VPN NAT用ローカルIPアドレス、ルータ部用VPN NAT用ローカルIPアドレスを復号化し、保持する。

【0129】1-12 端末サーバ部10は、VPNゲートウェイ5をIPsec対象ホストとしたPreshared Key、サーバ部用VPN NAT用ローカルIPアドレス、ルータ部用VPN NAT用ローカルIPアドレスの設定コマンド(ルータ部11のtelnetコマンドの実装により異なる)を作成する。この時、VPNゲートウェイのアドレスはダミーで設定する。

【0130】((コマンド送信処理))

1-13 前の処理で作成したコマンドをパラメータとして、端末(ルータ設定処理部102)から端末1(ルータ部11)へのtelnetコマンド<ローカルネットワークセッション>として、コマンドを送出する。

((端末ルータ部処理))

1-14 受信したPreshared Keyの設定及びVPN NAT110の設定をルータ部11に書き込む。

【0131】((レスポンス送信処理))

1-15 ステータス(正常またはエラーステータス(コマンド異常等))をパラメータとして、端末1(ルータ部11)から端末1(サーバ部10/コマンド送出処理部103)へのtelnetレスポンス<非IPsecセッション>としてレスポンスを送信する。

((端末ルータ設定部後処理))なし上記で設置通知処理が

完了となる。

【0132】<故障通知処理>図26のシーケンス図と図27の処理フローの手順図を示すよう、故障通知処理は、端末1が故障したことを検知し、保守サーバ3に通知する。端末1(サーバ部10)では、端末1のサーバ部10及びルータ部11の故障の発生、復旧を常時監視して、故障が発生したら故障通知処理を起動する。即ち、故障通知処理の①故障通知コマンド(端末ID、原文、MAC、故障コード)→②故障通知レスポンス→③リモートメンテナンス要求起動が行われる。

【0133】((通信契機))

7-1 端末1で故障発生を検知した場合、端末1が自律的に行う。

((端末前処理))

7-2 「端末1のユニークなID+タイムスタンプ」から認証のための原文を作成する。

7-3 原文に対して、Secret (ID2)を用いたメッセージ認証子(MAC)を生成する(ISO9797-1、ISO9797-2に準拠することが望ましい)。

【0134】((コマンド送信処理))

7-4 端末ID、原文、MAC、故障のコードをパラメータとして、端末1(サーバ部10/コマンド送出処理部103)から保守サーバ3(httpサーバ部30)へのhttpコマンドで<非IPsecセッション>として故障通知コマンドを送信する。

【0135】((保守サーバ処理))

7-5 保守サーバ3のhttpサーバ部30は、受信したコマンド名とパラメータをCGI処理部31に渡す。CGI処理部31は、原文に対して、Secret (ID2)を用いたメッセージ認証子(MAC)を生成して(端末1と同様の演算)、受信したMACと一致することを確認する(端末認証)。

7-6 CGI処理部31は、受信した故障コードを保持する。

【0136】((レスポンス送信処理))

7-7 保守サーバ3のhttpサーバ部30は、ステータス(正常またはエラーステータス(認証異常等))をパラメータとしたデータをCGI処理部31から受けて、保守サーバ3(httpサーバ部31)から端末1(サーバ部10/コマンド送出処理部103)へのhttpレスポンス<非IPsecセッション>としてレスポンスを送信する。

【0137】((端末後処理))

7-8 VPNGWアドレス要求処理を起動する。なお、故障通知処理によって保持した故障コードは、リモートメンテナンス装置4からhttpアクセス等で参照することが望ましい(故障確認処理)。

【0138】<VPNGWアドレス要求処理>図4のシーケンス図及び図14、図15の処理フロー手順のように、VPNGWアドレス要求は、保守サーバ3が選択し

た保守センタ9のVPNゲートウェイ5iのアドレスを情流GW端末1に通知することを主旨とする。基本的には、内線端末2a~2nから情流GW端末1にリモートメンテナンス要求の登録があった時点で、VPNGWアドレス要求が通知されるものの、端末管理者が情流GW端末1本体のボタン操作でVPNGWアドレス要求を通知することも可能とする。

【0139】①VPNGWアドレス要求コマンド（端末サーバ部10→保守サーバ3）
（通信契機）

9-1 内線端末2a~2nから情流GW端末1へのWEBアクセス又は端末管理者のボタン操作などによる情流GW端末1へのアクションによる。

【0140】（端末前処理）

9-2 内線端末2a~2nからのブラウザアクセスにより起動される場合は、リモートメンテナンス要求で必要な情報である「要求者名、要求者レベル、内線端末名（複数設定可）、緊急度、電話番号、要求内容」をブラウザから入力させることにより、取得し、リモートメンテナンス情報として保持する。画面イメージでは、ブラウザ画面の通りである。情流GW端末1のボタン操作により起動される場合は、「要求者名、要求者レベル、端末名、緊急度、電話番号、要求内容」を事前に登録されたテーブルから取得し、保持する。要求者レベルは、一般又は管理者を設定可能とする。尚、内線端末名は、リモートメンテナンス対象としたい内線端末の名称であり、他の情報は、保守センタ9のオペレータが、リモートメンテナンス要求を起動したユーザがセンタ9のオペレータにリモートメンテナンスを実施してもらうにあたり、その意向を示すための情報である。

【0141】9-3 サーバ部10のコマンド送出処理部103は、秘密鍵と公開鍵を生成する。アルゴリズムにはRSA等の公開鍵暗号を使用する。

9-4 「端末のユニークなID+タイムスタンプ」から認証のための原文を生成する。

9-5 原文に対して、Secret(id2)を用いたメッセージ認証子(MAC)を生成する。(ISO9797-1, ISO9797-2)に準拠することが望ましい。)

【0142】（コマンド送信処理）

9-6 端末ID, 原文, MAC, 公開鍵をパラメータとして、端末1（サーバ部10/コマンド送出処理部103）から保守サーバ3（httpサーバ部30）へのhttpコマンドで<非Ipsecセッション>としてリモートメンテナンス要求コマンドを送信する。

【0143】②VPNGW選択処理

（保守サーバ処理部）

9-7 保守サーバ3のhttpサーバ部30は、受信したコマンド名とパラメータをCGI処理部31に渡す。CGI処理部31は、原文に対して、Secret

(id2)を用いたメッセージ認証子(MAC)を生成して(端末1と同様の演算)、受信したMACと一致することを確認する。(端末認証)

【0144】9-8 保守サーバ3はVPNGWトンネルDBを読み出し、VPNGWトンネルDBの割り当て状況のトンネルを先頭から検索し、フィールドの値が「未使用」のトンネル番号を取得する。また、当該取得したトンネル番号に対応するフィールドを「未使用」から「端末ID」に書き換え、対応するVPNGWグローバルIPアドレスを取得する。以下、このグローバルIPアドレスに対応するVPNGWを「5i」とする。ここで示したVPNゲートウェイ5a~5nの選択処理は、本発明の特徴の一つである。

【0145】9-9 レスポンスのパラメータの前記「VPNGWグローバルIPアドレス」を受信した公開鍵で暗号化する。

【0146】③VPNGWアドレス要求レスポンス（保守サーバ3→端末サーバ部10）
（レスポンス送信処理）

9-10 保守サーバ3のhttpサーバ部30は、ステータス（正常又はエラーステータス（認証異常等））、端末1の公開鍵で暗号化したVPNGWグローバルIPアドレスをパラメータとしたデータをCGI処理部31から受けて、保守サーバ3（httpサーバ部30）から端末1（サーバ部10/コマンド送出処理部103）へのhttpレスポンス<非セッション>としてレスポンスを送信する。

【0147】④VPNGWアドレス要求レスポンス受信後処理（端末サーバ部10→端末ルータ部11）

（端末前処理）

9-11 端末サーバ部10は、端末1の秘密鍵で、VPNGWグローバルIPアドレスを復号化し、保持する。

【0148】9-12 端末サーバ部10は、VPNGWグローバルIPアドレスをVPN対向ホストとして設定するためのコマンド（ルータ部11のtelnetコマンドの実装により異なる。）を作成する。

9-13 前の処理で作成したコマンドをパラメータとして、端末1（ルータ設定処理部102）から端末1（ルータ部11）へのtelnetコマンド<ローカルネットワークセッション>として、コマンドを送出する。

【0149】（端末ルータ部処理）

9-14 VPNGWグローバルアドレスをVPN対向ホストとする設定をルータ部11に書き込む。

（レスポンス送信処理）

9-15 ステータス（正常又はエラーステータス（コマンド異常等））をパラメータとして、端末1（ルータ部11）から端末1（サーバ部10/コマンド送出処理部103）へのtelnetレスポンス<非Ipsec

セッション>としてレスポンスを送信する。

【0150】(端末ルータ設定部後処理)

9-16 リモートメンテナンス要求処理を起動する。
以上によりVPNGWアドレス要求処理が完了となる。
この本処理が発明のポイントの一つである。

【0151】<リモートメンテナンス要求処理>図5のシーケンス図と図16乃至図19の処理フローの手順図に示すよう、リモートメンテナンス要求処理は、IPsecによるリモートメンテナンスの実施を保守サーバ3に要求することを主旨とする。

【0152】また、リモートメンテナンス要求処理では、VPNを構築するための情流GW端末1のIPアドレスをセンタ9に通知することも主旨の一つである。リモートメンテナンス要求は、httpプロトコルで行われその環境変数から、保守サーバ3は、情流GW端末1に受信したIPアドレスを取得する。そのIPアドレスをもとに保守センタ9のVPNゲートウェイ5iに対して、VPN鍵、端末IPアドレスを設定する。

【0153】更に、VPNを構築する際、各情流GW端末1配下の内線端末2a~2nに対してIPレベルの通信を行えるようにするために、センタ9からリモートメンテナンス対象内線端末2a~2nに対するVPNNAT用ローカルIPアドレスを取得し、VPNNAT処理を行う。

【0154】VPNNAT処理を行うことにより、情流GW端末1配下のローカルLANアドレスが同一である複数の情流GW端末1へのメンテナンスを行う場合でも(例えば、メンテナンス対象の情流GW端末1が二つ存在し、二つの情流GW端末1が共に192.168.0.0/24のローカルネットを持つような場合)、保守センタ9のオペレータ端末から情流GW端末1及びその配下の内線端末2a~2nに対してIPリチャールな環境を構築できる。

【0155】①リモートメンテナンス要求コマンド(端末サーバ部10→保守サーバ3)

((通信契機))

2-1 VPNGWアドレス要求の処理終了後に、起動される。

【0156】((端末前処理))

2-2 VPNGWアドレス要求で保持したリモートメンテナンス情報を取得する。

【0157】2-3 サーバ部10のコマンド送出処理部103は、秘密鍵と公開鍵を生成する。アルゴリズムにはRSA等の公開鍵暗号を使用する。

2-4 「端末1のユニークなID+タイムスタンプ」から認証のための原文を作成する。

【0158】2-5 原文に対して、Secret(ID2)を用いたメッセージ認証子(MAC)を生成する(ISO9797-1、ISO9797-2に準拠することが望ましい)。

2-6 保守センタ9に通知するためのパラメータのう

ち、「要求者名、内線端末名、電話番号、要求内容」を情流GW端末1に保持されているSecret(ID2)で暗号化する。

【0159】((コマンド送信処理))

2-7 端末ID、原文、MAC、公開鍵、要求者レベル、緊急度、暗号化要求者名、暗号化内線端末名(複数可)、暗号化電話番号、暗号化要求内容をパラメータとして、端末1(サーバ部10/コマンド送出処理部103)から保守サーバ3(httpサーバ部30)へのhttpコマンドで<非IPsecセッション>としてリモートメンテナンス要求コマンドを送信する。

【0160】②VPNNAT用ローカルIPアドレス割り当て処理

((保守サーバ処理))

2-8 保守サーバ3のhttpサーバ部30は、受信したコマンド名とパラメータをCGI処理部31に渡す。CGI処理部31は、原文に対して、Secret(ID2)を用いたメッセージ認証子(MAC)を生成して(端末と同様の演算)、受信したMACと一致することを確認する(端末認証)。

【0161】2-9 CGI処理部31は、受付番号を生成し、リモートメンテナンス要求DB92のレコードを新規にクリエイトし、受付番号、受信時刻、メンテナンス状態(この時点では、常に対応待ち)を保守端末ブラウザの端末DB90に保持する。また、テーブル名には、要求者レベルが管理者の場合は、「管理者」として保持し、要求者レベルが一般の場合は、内線端末2a~2n名を保持する。なお、端末DB90のレコードを図26に示す。

【0162】2-10 CGI処理部31は、環境変数REMOTE_ADDRから情流GW端末1のグローバルIPアドレスを取得し、前記リモートメンテナンス要求DB92のレコードに保持する。

2-11 CGI処理部31は、端末ID、要求者レベル、緊急度を前記リモートメンテナンス要求DB92のレコードに保持する。

【0163】2-12 CGI処理部31は、暗号化内線端末名、暗号化要求者名、暗号化電話番号、暗号化要求内容をSecret(ID2)で復号化し前記リモートメンテナンス要求DB92のレコードに保持する。なお、リモートメンテナンス要求DB92のレコードを図27に示す。

【0164】2-13 CGI処理部31は、通知された端末ID/内線端末名(複数端末名が存在する場合は、それぞれの端末名について)をキーとして、VPNNATDB91を検索し、その端末1にVPNNAT用ローカルIPアドレスが割り当てられているかどうかを判断する。

【0165】VPNNAT用ローカルIPアドレスが割り当てられていれば、割り当て済みのVPNNAT用ロ

ーカルIPアドレスを前記リモートメンテナンス要求DB92のレコードに保持し、VPN NAT用ローカルIPアドレスが割り当てられていなければ、VPN NAT DB91から空きVPN NAT用ローカルIPアドレスを選択する。

【0166】該当レコードの割り当て状況フィールドに情流GW端末ID／内線端末名を保持するとともに、保持したVPN NAT用ローカルIPアドレスを前記リモートメンテナンス要求DB92のレコードにも保持する。なお、VPN NAT DB91のレコードを図30に示す。

【0167】2-14 CGI処理部31は、リモートメンテナンス装置4のWEBブラウザ上に、リモートメンテナンス要求を受信した旨を表示できるようにページを作成する。表示内容は、受付番号、端末ID、グローバルIPアドレス、要求者名、要求者レベル、電話番号、緊急度、要求内容、受信時刻、VPN NAT用ローカルIPアドレス、テーブル名、メンテナンス状態を表示する(図29参照)。

【0168】㊟リモートメンテナンス要求レスポンス処理(保守サーバ3→端末サーバ部10)

(保守サーバ部)

2-26 レスポンス処理の内、「内線端末名とダミーIPアドレスの組」を受信した公開鍵で暗号化する。

(レスポンス送信処理)

2-27 保守サーバ3のhttpサーバ部30は、ステータス(正常又はエラーステータス(認証異常等))、受付番号、端末1の公開鍵で暗号化した内線端末名とVPN NAT用ローカルIPアドレスの組(複数可)をパラメータとしたデータをCGI処理部31から受けて、保守サーバ3(httpサーバ部30)から端末1(サーバ部10/コマンド送出処理部103)へのhttpレスポンス<非IPsecセッション>としてレスポンスを送信する。

【0169】㊿IPsec処理対象パケット設定(保守センタ9→VPNゲートウェイ5i)

(コマンド送信処理)

2-15 VPNゲートウェイ設定処理部32は、リモートメンテナンス要求DBの該当レコードから、端末IDおよび㊿の処理で保持したVPN NAT用ローカルIPアドレス向けパケットを取得する。

2-16 VPNゲートウェイ設定処理部32は、VPN NAT用ローカルIPアドレス向けパケットを端末IDに対応したVPNトンネル12に割り付けるための設定(VPNゲートウェイ5iのtelnetコマンドの実装により異なる。)をパラメータとして、保守サーバ3(VPNゲートウェイ設定処理部32)からVPNゲートウェイ5i(設定コマンド受信処理部51)へのtelnetコマンド<ローカルネットワークセッション>としてコマンドを送信する。

【0170】(VPNゲートウェイ処理)

2-17 受信したVPN NAT用ローカルIPアドレスをIPsec処理対象ホストとするための設定をVPNゲートウェイ5iに書き込む。

(レスポンス送信処理)

2-18 ステータス(正常又はエラーステータス(コマンド異常など))をパラメータとして、VPNゲートウェイ5i(設定コマンド受信処理部51)から保守サーバ3(VPNゲートウェイ設定処理部32)へのtelnetレスポンス<ローカルネットワークセッション>としてレスポンスを送信する。

【0171】(VPNゲートウェイ設定処理部後処理)

2-19 VPNゲートウェイ設定処理部32は、「㊿リモートメンテナンス要求コマンド」で受信した端末IDを持つ情流GW端末1との間にVPNが確立しているかをVPNゲートウェイ5iから取得する。

2-20 VPNゲートウェイ5iのVPN確立状況より、VPNが確立している場合は、プロセスを終了する。VPNが確立していない場合は、㊿IPsec設定処理を起動する。

【0172】㊿IPsec設定処理(保守センタ9→VPNゲートウェイ5i)

(VPNゲートウェイ設定処理部前処理)

2-21 保守サーバ3/CGI処理部31からIPsecの認証鍵(PresharedKey)、端末ルータ部11のグローバルIPアドレスを取得し、コマンドを生成する。

【0173】(コマンド送信処理)

2-22 端末ルータ部11のグローバルIPアドレスをIPsec対象ホストとしたPresharedkeyの設定及び端末IDに対応したVPNトンネル12を確立するための設定(VPNゲートウェイ5iのtelnetコマンドの実装により異なる。)をパラメータとして、保守サーバ3(VPNゲートウェイ設定処理部32)からVPNゲートウェイ5i(設定コマンド受信処理部51)へのtelnetコマンド<ローカルネットワークセッション>としてコマンドを送信する。

【0174】(VPNゲートウェイ処理)

2-23 受信したPresharedkey及びVPNトンネル12を確立するための設定をVPNゲートウェイ5iに書き込む。

(レスポンス送信処理)

2-24 ステータス(正常又はエラーステータス(コマンド異常など))をパラメータとして、VPNゲートウェイ5i(設定コマンド受信処理部51)から保守サーバ3(VPNゲートウェイ設定処理部32)へのtelnetレスポンス<ローカルネットワークセッション>としてレスポンスを送信する。

【0175】(保守サーバ後処理)

2-25 VPNゲートウェイ設定処理部32は、「㊿

リモートメンテナンス要求コマンド」で受信した端末IDを持つ情流GW端末1との間にVPNの確立が完了しているかをVPNゲートウェイiから取得する。確立が完了していない場合は、数秒間隔でVPN確立の完了を確認するまで同様の取得処理を繰り返す。VPNの確立完了が確認できた時点で、⑤リモートメンテナンス要求レスポンス処理を起動する。尚、VPN設定が完了した段階で、その状態が、リモートメンテナンス装置4から確認できることが望ましい。理由は、VPN設定が完了したことを確認した上で、⑥リモートメンテナンス開始指示を行えた方が保守者の作業効率がよいからである。

【0176】⑥サーバ部10とルータ部11のVPN NAT設定（端末サーバ部10→端末ルータ部11）（端末処理部）

2-28 リモートメンテナンス要求レスポンスを受信した端末サーバ部10は、受付番号を保持する。

2-29 端末サーバ部10は、端末1の秘密鍵で、内線端末名とVPN NAT用ローカルIPアドレスの組（複数の場合あり）を復号化し、ホストテーブルに保持する。

【0177】2-30 端末サーバ部10は、内線端末名をキーとして、端末サーバ部10がもっている内線端末名と実IPアドレスの組のテーブル（DNSなどで参照）から端末名に対応する実IPアドレスを取得し、端末名に対応するVPN NAT用ローカルIPアドレスと実IPアドレスをVPN NAT110で対応付ける設定コマンド（複数の場合あり）（ルータ部11のtelnetコマンドの実装により異なる。）を作成する。

（コマンド送信処理）

2-31 2-30で作成したコマンドをパラメータとして、端末1（ルータ設定処理部102）から端末1（ルータ部11）へのtelnetコマンド<ローカルネットワークセッション>として、コマンドを送出する。

【0178】（端末ルータ部処理）

2-32 VPN NAT110の設定をルータ部11に書き込む。

（レスポンス送信処理）

2-33 ステータス（正常又はエラーステータス（コマンド異常等））をパラメータとして、端末1（ルータ部11）から端末1（サーバ部10/コマンド送出処理部102）へのtelnetレスポンス<非Ipsecセッション>としてレスポンスを送信する。

（端末ルータ設定部後処理）なし

以上により、リモートメンテナンス要求処理が完了となる。

【0179】<リモートメンテナンス実施処理>

（リモートメンテナンス装置4→内線端末2a～2n）

図6のシーケンス図及び図19の手順フロー図に示すよ

うに、リモートメンテナンス実施処理は、前記リモートメンテナンス要求処理を受けて、Ipsec等のVPNによるトンネル12を経由してリモートメンテナンス装置4から情流GW端末1本体及びその内線端末2a～2nに対してセキュアなリモートメンテナンスを行い（VPN経由で行うため、伝送路が暗号化できる）、端末1の故障の復旧、パソコンへのアプリケーションのリモートインストール等を実施することを主旨とする。

【0180】リモートメンテナンス装置4は、特殊なものではなく、ローカルネットワーク8上で内線端末2a～2nに対してコマンドを送出することにより、内線端末2a～2nをメンテナンスできる装置であればそれを転用できる。機能としては、故障（例えば、Proxy故障）について、復旧動作（proxyの起動、端末1の再起動）を行い故障を復旧する。また、端末1のログの表示や、ルータ部11の設定の確認も行える。ツールとしては、httpクライアント（Webブラウザ）や、telnetツール等である。

【0181】また、パソコンに対するリモートインストールについては、VNC等の遠隔制御ソフト等による。従って、この処理は、リモートメンテナンス装置4から、メンテナンスを行う内線端末2a～2nへの通信プロトコルに依存した汎用的なものであるため、詳しくは言及しない。

【0182】繰り返しになるが、センタ9から内線端末2a～2nへの接続は、リモートメンテナンス要求時に付与したVPN NAT用ローカルIPアドレスに対して行うことが本実施形態例のポイントである。

【0183】⑦リモートメンテナンス開始処理（リモートメンテナンス装置4→保守サーバ3）

（通信契機）VPNトンネル12が張られている状態において、リモートメンテナンス装置4（図中保守端末）上のWEBブラウザから、リモートメンテナンス保守者の任意の契機で起動される（前述した故障確認処理で故障を検知した時点でも、それに同期して起動するのが望ましい）。

【0184】（リモートメンテナンス開始処理）

3-1 保守サーバ3のリモートメンテナンス要求確認画面にアクセスし、対象とするリモートメンテナンス要求に対するリモートメンテナンスを開始したことをCGI処理部31で、保守サーバ3に通知する。

【0185】（サーバ処理）

3-2 CGI処理部31でリモートメンテナンス開始を起動されると、リモートメンテナンス要求DB92の該当テーブルのメンテナンス状態が「対応中」となる。

【0186】⑧リモートメンテナンス実施処理（リモートメンテナンス装置4→内線端末2a～2n）

（リモートメンテナンス実施）

3-3 リモートメンテナンスを実施する。リモートメンテナンスでは、リモートメンテナンス要求を受けたV

VPN NAT用ローカルIPアドレスに対してVPN経由でIP接続を行う。リモートメンテナンス実施時には、リモートメンテナンス要求DB92を参照しながら作業を行えるようにサーバ側のユーザインタフェースを設計することを強く推奨する。

【0187】<リモートメンテナンス終了処理>図7のシーケンス図と図20の手順フロー図に示すよう、リモートメンテナンス終了処理は、リモートメンテナンス要求で要求されたリモートメンテナンス作業が終了したことを、保守サーバ3から情流GW端末1に伝えることを主旨とする。

【0188】⑩リモートメンテナンス終了コマンド送信処理（保守サーバ3→端末サーバ部10）
（（通信契機））

4-1 VPNトンネル12が張られている状態において、要求されたリモートメンテナンス作業が終了した時点で、リモートメンテナンス装置4上のWEBブラウザから保守サーバ3に対するリモートメンテナンス保守者によるCGI処理部31のキックで起動される。

【0189】（（サーバ前処理））

4-2 CGI処理部31でリモートメンテナンス終了を起動されると、リモートメンテナンス要求DB92の該当テーブルのメンテナンス状態が「終了」となる。なお、図31にリモートメンテナンス要求DB92のテーブルレコードを示す。

【0190】4-3 保守サーバ3は、リモートメンテナンス要求DB92の該当テーブルのメンテナンス状態が「終了」となったこと検知すると、受付番号をパラメータとして、該当テーブルの受付番号を取得し、受付番号をパラメータとしてリモートメンテナンス終了コマンドを作成する。この受付番号は、後に説明するVPN NAT110解放処理及びVPN終了処理でも参照される。

【0191】（（コマンド送信処理））

4-4 前の処理で作成したコマンドをパラメータとして保守サーバ3から端末1（httpサーバ部100）へのhttpコマンドで<IPsecセッション>としてリモートメンテナンス終了コマンドを送信する。

【0192】⑪リモートメンテナンス終了コマンド受信処理（端末サーバ部10→保守サーバ3）
（（端末サーバ部処理））

4-5 リモートメンテナンス終了を受信すると、パラメータから受付番号を抽出し、保持していた受付番号の状態を終了とする。

【0193】（（レスポンス送信処理））

4-6 端末1のhttpサーバ部100は、ステータス（正常またはエラーステータス）をパラメータとし、端末1（httpサーバ部100）から保守センタ9へのhttpレスポンス<IPsecセッション>としてレスポンスを送信する。

【0194】⑫リモートメンテナンス終了レスポンス受信後処理（保守サーバ3）
（（サーバ後処理））

4-7 レスポンス受信後、該当内線端末2a～2nに対するメンテナンスが全て終了したかを判断し、該当内線端末2a～2nに対するメンテナンスが全て終了していなかったら処理を終了する。該当内線端末2a～2nに対するメンテナンスが全て終了していたら、さらに、終了した内線端末は情流GW端末1のサーバ部10又はルータ部11かを判断し、端末1のサーバ部10又はルータ部11でない場合は、VPN NAT解放処理を起動する。

【0195】端末1のサーバ部10又はルータ部11の場合は、対応する情流GW端末1に対するリモートメンテナンスを全て終了したかを判断し、全て終了していたら、VPN終了処理を起動し、全て終了していなかったら、処理を終了する。以上で、リモートメンテナンス終了処理が完了となる。

【0196】<VPN NAT解放処理>図8のシーケンス図及び図21、図22の手順フロー図に示すよう、VPN NAT110解放処理は、リモートメンテナンス要求時に保守センタ9から情流GW端末1に割り振られたVPN NAT用のVPN NAT用ローカルIPアドレスを解放することを主旨とする。

【0197】⑬VPN NAT110解放コマンド送信処理（保守サーバ3→端末サーバ部10）
（（通信契機））

5-1 VPNトンネル12が張られている状態において、リモートメンテナンス終了後、該当内線端末2a～2nに対するメンテナンスが全て終了し、その内線端末2a～2nが情流GW端末1のサーバ部10又はルータ部11以外の場合に起動される。

【0198】（（サーバ前処理））

5-2 VPN NAT110解放コマンドを作成する。なお、リモートメンテナンス要求DB92のテーブルレコードは図31と同一である。
（（コマンド送信処理））

5-3 保守サーバ3は、内線端末名をパラメータとして、保守サーバ3から端末1（httpサーバ部100）へのhttpコマンドで<IPsecセッション>としてVPN NAT解放コマンドを送信する。

【0199】⑭VPN NAT解放コマンド受信処理（端末サーバ部10→端末ルータ部11）
（（端末前処理））

5-4 端末サーバ部10は、VPN NAT110解放コマンドを受信し、パラメータの内線端末2a～2n名をキーとして、端末サーバ部10がもっている端末名と実IPアドレスの組のテーブル（DNS等で参照）から端末名に対応する実IPアドレスを取得する。

【0200】そして、端末名に対応するVPN NAT用

ローカルIPアドレスと実IPアドレスのVPN NAT 110を解放するコマンド（複数の場合あり）（ルータ部11のtelnetコマンドの実装により異なる）を作成する。

【0201】((コマンド送信処理))

5-5 前の処理で作成したコマンドをパラメータとして、端末1（ルータ設定処理部102）から端末1（ルータ部11）へのtelnetコマンド<ローカルネットワークセッション>として、コマンドを送出する。

((端末ルータ部処理))

5-6 VPN NAT 110解放の設定をルータ部11に書き込む。

【0202】((レスポンス送信処理))

5-7 ステータス（正常またはエラーステータス（コマンド異常等））をパラメータとして、端末1（ルータ部11）から端末1（サーバ部10/コマンド送出処理部103）へのtelnetレスポンス<非IPsecセッション>としてレスポンスを送信する。

((端末ルータ設定部後処理))

5-8 ホストテーブルの端末名に対応するレコードを削除する。

【0203】㊸VPN NAT 110解放レスポンス送信処理（端末サーバ部10→保守サーバ3）

((レスポンス送信処理))

5-9 端末1のhttpサーバ部100は、ステータス（正常またはエラーステータス）をパラメータとし、端末1（サーバ部10）から保守センタ9へのhttpレスポンス<IPsecセッション>としてレスポンスを送信する。

【0204】㊹保守サーバ側VPN NAT用ローカルIPアドレス変換処理（保守サーバ3）

((VPN NAT用ローカルIPアドレス変換処理))

5-10 サーバ側で処理中の受付番号に対応する内線端末2a~2nに対応するVPN NAT用ローカルIPアドレスをリモートメンテナンス要求DB92から取得し、保持するとともに、VPN NAT DB91の対応VPN NAT用ローカルIPアドレスを解放する。

【0205】㊺IPsec処理対象パケット解除設定（保守サーバ3→VPNゲートウェイ5）

((コマンド送信処理))

5-11 VPNゲートウェイ設定処理部32は、リモートメンテナンス要求DB92の処理中の受付番号に該当するレコードから、端末ID、VPN NAT用ローカルIPアドレスを取得する。

【0206】5-12 VPNゲートウェイ設定処理部32は、VPN NAT用ローカルIPアドレス向けパケットを端末IDに対応したVPNトンネル12に割り付けるための設定を解除するためのコマンド（VPNゲートウェイ5のtelnetコマンドの実装により異なる）をパラメータとして、保守サーバ3（VPNゲート

ウェイ設定処理部32）からVPNゲートウェイ5（設定コマンド受信処理部51）へのtelnetコマンド<ローカルネットワークセッション>としてコマンドを送信する。

【0207】((VPNゲートウェイ処理))

5-13 受信したVPN NAT用ローカルIPアドレス向けルーティングの設定をVPNゲートウェイ5から解除する。

【0208】((レスポンス送信処理))

5-14 ステータス（正常またはエラーステータス（コマンド異常等））をパラメータとして、VPNゲートウェイ5（設定コマンド受信処理部51）から保守サーバ3（VPNゲートウェイ設定処理部32）へのtelnetレスポンス<ローカルネットワークセッション>としてレスポンスを送信する。

【0209】((VPNゲートウェイ設定処理部後処理))

5-15 対応する情流GW端末1に対するリモートメンテナンスを全て終了したかを判断し、全て終了していたら、VPN終了処理を起動し、全て終了していなかったら、処理を終了する。

【0210】<VPN終了処理>図9のシーケンス図及び図23乃至図25の手順フロー図に示すよう、VPN終了処理は、リモートメンテナンス要求時に保守センタ9から構築されたVPNを終了することを主旨とする。

【0211】㊻VPN終了コマンド送信処理（保守サーバ3→端末サーバ部10）

((通信契機))

6-1 VPNトンネル12が張られている状態において、リモートメンテナンス終了後、対応する情流GW端末1に対するメンテナンスが全て終了した場合に起動される。

【0212】((サーバ前処理))

6-2 VPN終了コマンドを作成する。なお、リモートメンテナンス要求DB92のテーブルレコードは図29と同一である。

((コマンド送信処理))

6-3 保守サーバ3は、保守サーバ3から端末1（httpサーバ部100）へのhttpコマンドで<IPsecセッション>としてVPN終了コマンドを送信する。

【0213】㊼VPN終了コマンド受信処理（端末サーバ部10→端末ルータ部11）

((端末前処理))

6-4 端末サーバ部10は、VPN終了コマンドを受信し、全てのVPN NAT 110を解放するコマンド（複数の場合あり）（ルータ部11のtelnetコマンドの実装により異なる）を作成する。

【0214】((コマンド送信処理))

6-5 前の処理で作成したコマンドをパラメータとして、端末1（ルータ設定処理部102）から端末1（ル

ータ部11)へのtelnetコマンド<ローカルネットワークセッション>として、コマンドを送出する。

③VPN NAT設定初期化コマンド受信及び処理(ルータ部11)

((端末ルータ部処理))

6-6 VPN NAT 110解放の設定をルータ部11に書き込む。

【0215】((レスポンス送信処理))

6-7 ステータス(正常またはエラーステータス(コマンド異常等))をパラメータとして、端末1(ルータ部11)から端末1(サーバ部10/コマンド送出処理部103)へのtelnetレスポンス<ローカルセッション>としてレスポンスを送信する。

((端末ルータ設定部後処理))

6-8 ホストテーブルを全て削除する。

【0216】④VPN終了レスポンス送信処理(端末サーバ部10→保守サーバ11)

((レスポンス送信処理))

6-9 端末1のhttpサーバ部100は、ステータス(正常またはエラーステータス)をパラメータとし、端末1(httpサーバ部100)から保守センタ9へのhttpレスポンス<IPsecセッション>としてレスポンスを送信する。

【0217】⑤保守サーバ側VPN NAT用ローカルIPアドレス変換処理(保守サーバ3)

((VPN NAT用ローカルIPアドレス変換処理))

6-10 サーバ側で処理中の受付番号に対応するVPN NAT用ローカルIPアドレスを全てリモートメンテナンス要求DB92から取得し、保持するとともに、VPN NAT DB91の対応VPN NAT用ローカルIPアドレスを解放する。

【0218】⑥IPsec処理対象パケット解除設定(保守サーバ3→VPNゲートウェイ5)

((コマンド送信処理))

6-11 VPNゲートウェイ設定処理部32は、リモートメンテナンス要求DB92の該当レコードから、端末IDに対応するすべての端末ID、VPN NAT用ローカルIPアドレスを取得する。

【0219】6-12 VPNゲートウェイ設定処理部32は、VPN NAT用ローカルIPアドレス向けパケットを端末IDに対応したVPNトンネル12に割り付けるための設定を解除するためのコマンド(VPNゲートウェイ5のtelnetコマンドの実装により異なる)をパラメータとして、保守サーバ3(VPNゲートウェイ設定処理部32)からVPNゲートウェイ5(設定コマンド受信処理部51)へのtelnetコマンド<ローカルネットワークセッション>としてコマンドを送信する。

【0220】((VPNゲートウェイ処理))

6-13 受信したVPN NAT用ローカルIPアドレ

ス向けルーティングの設定をVPNゲートウェイ5から解除する。

【0221】((レスポンス送信処理))

6-14 ステータス(正常またはエラーステータス(コマンド異常等))をパラメータとして、VPNゲートウェイ5(設定コマンド受信処理部51)から保守サーバ3(VPNゲートウェイ設定処理部32)へのtelnetレスポンス<ローカルネットワークセッション>としてレスポンスを送信する。

【0222】⑦IPsec設定解除コマンド送信処理(保守サーバ3→VPNゲートウェイ5)

((コマンド送信処理))

6-15 VPNゲートウェイ設定処理部32は、処理中の受付番号に対応するリモートメンテナンス要求DB92のレコードから、端末IDを取得する。

【0223】6-16 VPNゲートウェイ設定処理部32は、端末IDに対応したVPNトンネル12を解除するための設定(VPNゲートウェイ5のtelnetコマンドの実装により異なる)をパラメータとして、保守サーバ3(VPNゲートウェイ設定処理部32)からVPNゲートウェイ5(設定コマンド受信処理部51)へのtelnetコマンド<ローカルネットワークセッション>としてコマンドを送信する。

【0224】⑧IPsec設定解除コマンド受信及び処理(VPNゲートウェイ5)

((VPNゲートウェイ処理))

6-17 受信した端末IDに対応するVPNの設定をVPNゲートウェイ5から解除する。

【0225】((レスポンス送信処理))

6-18 ステータス(正常またはエラーステータス(コマンド異常等))をパラメータとして、VPNゲートウェイ5(設定コマンド受信処理部51)から保守サーバ3(VPNゲートウェイ設定処理部32)へのtelnetレスポンス<ローカルネットワークセッション>としてレスポンスを送信する。

【0226】((VPNゲートウェイ設定処理部後処理))

6-19 VPNGWアドレス要求処理でVPNゲートウェイトンネルDBから取得保持し「端末ID」を書き込んだフィールドを「未使用」に書き換え、VPNトンネルリソースを解放する。

上記でリモートメンテナンス終了処理が完了となる。以上、シーケンス図3～シーケンス図9及び手順フロー図13～手順フロー図25をもとに、リモートメンテナンスの処理手順を説明した。

【0227】本記録媒体例は、当該リモートメンテナンスの処理プログラム手順の一連の完結手続をコンピュータ読取り自在に実録したものである。

【0228】本実施形態例では、情流GW端末1本体のサーバ部10及びルータ部11へのVPN NAT 110の設定は設置通知時に行っているが、これはリモートメ

メンテナンス要求なしに、保守センタ側から任意の契機で情流GW端末1にVPNアクセスを可能とするための機能である。したがって、情流GW端末1本体のサーバ部10及びルータ部11へのVPNNAT110の設定を特別扱いせずに、リモートメンテナンス要求時にVPNNAT110を設定し、それをVPNNAT110解放時に解放する手順でもよいのは言うまでもない。

【0229】本実施例においては、VPNにIPsecを用いて説明しているが、本発明はレイヤ3レベルのVPNであればIPsec以外に対しても適用可能なことは言うまでもない。

【0230】

【発明の効果】かくして、本発明によれば、VPNNATに用いる有限のVPNNAT用ローカルIPアドレスリソースが、リモートメンテナンス要求端末に対してだけ割り当てられて、リモートメンテナンス終了時にVPNNAT解放プロセスで解放されることにより、IPアドレス資源が節約でき、静的VPNNAT方式と比較して同時に多くの端末をリモートメンテナンスできる。

【0231】言い換えれば、従来は最大「VPNNAT用ローカルIPアドレスリソース」分の内線端末をリモートメンテナンス対象端末となっていたのに対し、本発明を用いることにより、同時に「VPNNAT用ローカルIPアドレスリソース」分の内線端末をリモートメンテナンス対象端末とすることが可能になり、リモートメンテナンスサービス対象端末の加入者数を大幅に増やすことができる。

【0232】しかも、VPNNATに用いる有限のVPNNAT用ローカルIPアドレスリソースが、リモートメンテナンス要求端末に対してだけ割り当てられて、リモートメンテナンス終了時にVPNNAT解放プロセスで解放されることにより、リモートメンテナンス要求対象とした内線端末に対してだけ保守センタからのアクセスを許すリモートメンテナンス方法を実現することができる。

【0233】また、リモートメンテナンスサービス提供者にとっては、保守センタがVPNゲートウェイの設備を設置する際、VPNリモートメンテナンスのアクセス数に応じてVPNゲートウェイの設備を増設設置することができ、ひいては、VPNゲートウェイの設備コストを最適化できる。

【0234】前述の効果から、リモートメンテナンスサービスを楽しむお客様にとっては、保守センタとVPNを構築する際VPNのリソース不足となることが少なくなり、VPN構築失敗でリモートメンテナンスを受けられなくなるケースが減少する。

【図面の簡単な説明】

【図1】本発明の実施の形態を示すシステム例のシステム構成図である。

【図2】同上において、VPNNATに動的にVPNNAT用ローカルIPアドレスを付与する機能説明図であ

る。

【図3】本発明の実施の形態を示す方法例における設置通知処理のシーケンス図である。

【図4】同上におけるVPNGWアドレス要求処理のシーケンス図である。

【図5】同上におけるリモートメンテナンス要求処理のシーケンス図である。

【図6】同上におけるリモートメンテナンス実施処理のシーケンス図である。

【図7】同上におけるリモートメンテナンス終了処理のシーケンス図である。

【図8】同上におけるVPNNAT解放処理のシーケンス図である。

【図9】同上におけるVPN終了処理のシーケンス図である。

【図10】本発明の実施の形態を示すプログラム例及び記録媒体例における情報GW端末側概括フローチャートである。

【図11】同上における保守センタ側概括フローチャートである。

【図12】同上における設置通知処理の前半フロー手順図である。

【図13】同上における設置通知処理の後半フロー手順図である。

【図14】同上におけるVPNGWアドレス要求処理の前半フロー手順図である。

【図15】同上におけるVPNGWアドレス要求処理の後半フロー手順図である。

【図16】同上におけるリモートメンテナンス要求処理の初期段階フロー手順図である。

【図17】同上におけるリモートメンテナンス要求処理の第2段階フロー手順である。

【図18】同上におけるリモートメンテナンス要求処理の最終段階フロー手順図である。

【図19】同上におけるリモートメンテナンス実施処理のフロー手順図である。

【図20】同上におけるリモートメンテナンス終了処理のフロー手順図である。

【図21】同上におけるVPNNAT解放処理の前半フロー手順図である。

【図22】同上におけるVPNNAT解放処理の後半フロー手順図である。

【図23】同上におけるVPN終了処理の初期フロー手順図である。

【図24】同上におけるVPN終了処理の中間フロー手順図である。

【図25】同上におけるVPN終了処理の最終フロー手順図である。

【図26】本発明の実施の形態を示す方法例における故障通知処理のシーケンス図である。

【図27】本発明の実施の形態を示すプログラム例及び記録媒体例における故障通知処理のフロー手順図である。

【図28】図16中、端末DB90のレコード内容を示すテーブルである。

【図29】図16中、リモートメンテナンス要求DB92のレコード内容を示すテーブルである。

【図30】図16中、VPN NAT DB91のレコード内容を示すテーブルである。

【図31】図20中、リモートメンテナンス要求DB92のレコード内容を示すテーブルである。

【図32】従来システムにおけるVPN NATの機能説明図である。

【図33】同上における2地点同時接続のVPN NATの機能説明図である。

【符号の説明】

1…インターネットゲートウェイ端末（端末情報GW端末）

2a～2n…内線端末

3…保守サーバ

4…リモートメンテナンス装置

5、5a、5i、5n…VPNゲートウェイ（VPNGW）

6…インターネット

7、8…ローカルネットワーク（LAN）

9…保守センタ（センタ）

10…サーバ部（端末サーバ部）

11…ルータ部（端末ルータ部、VPNルータ部）

12…VPNトンネル

30、100…httpサーバ部

31、101…CGI処理部

32…VPNゲートウェイ設定処理部

40…メンテナンスコマンド処理部

50…VPN処理部

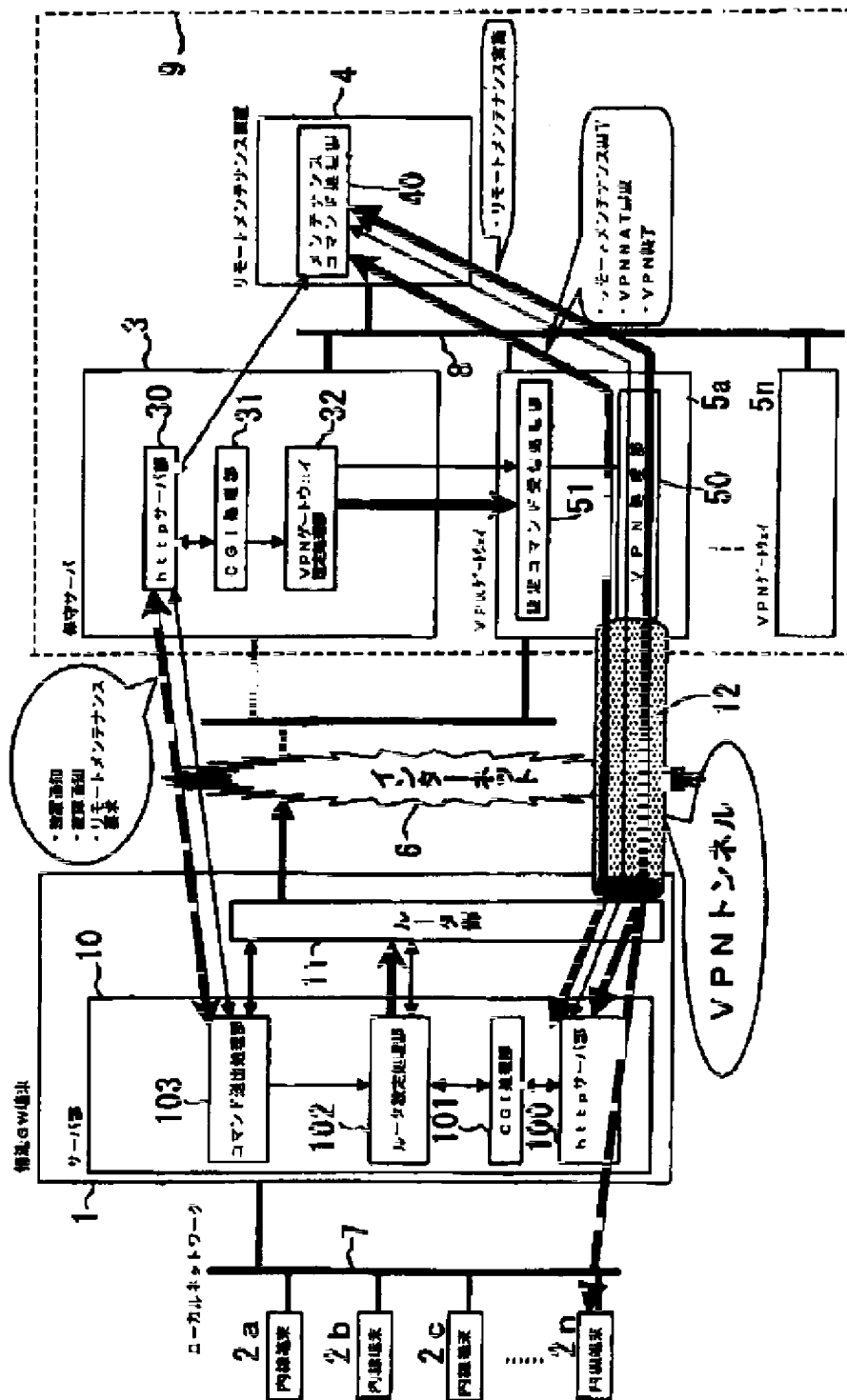
51…設定コマンド受信処理部

102…ルータ設定処理部

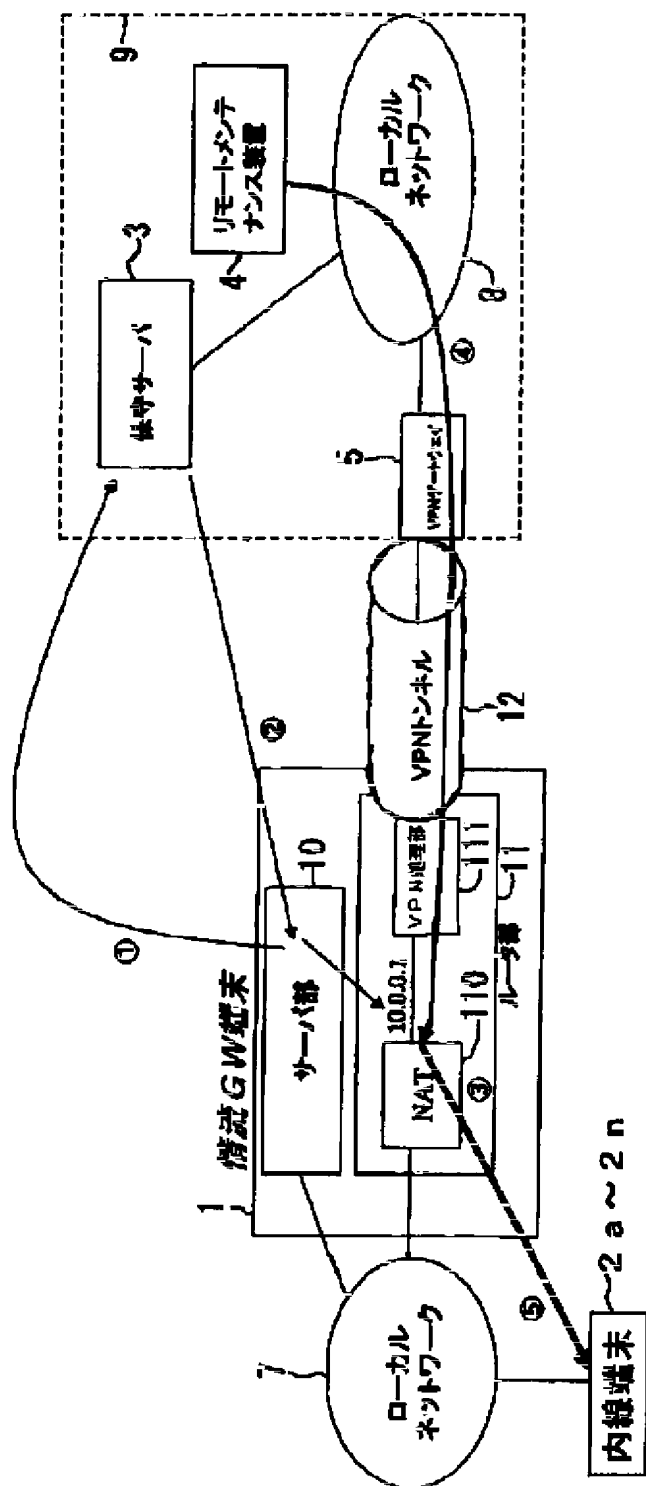
103…コマンド送出処理部

110…NAT（VPN NAT）

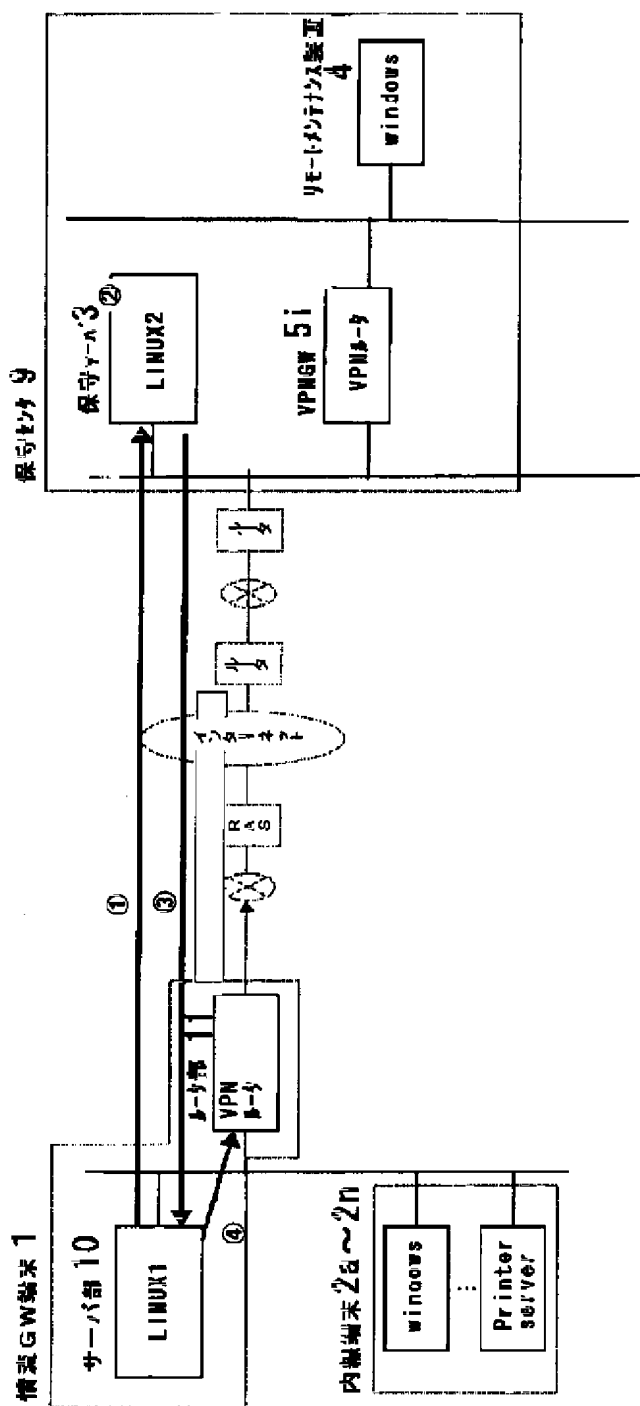
【図1】



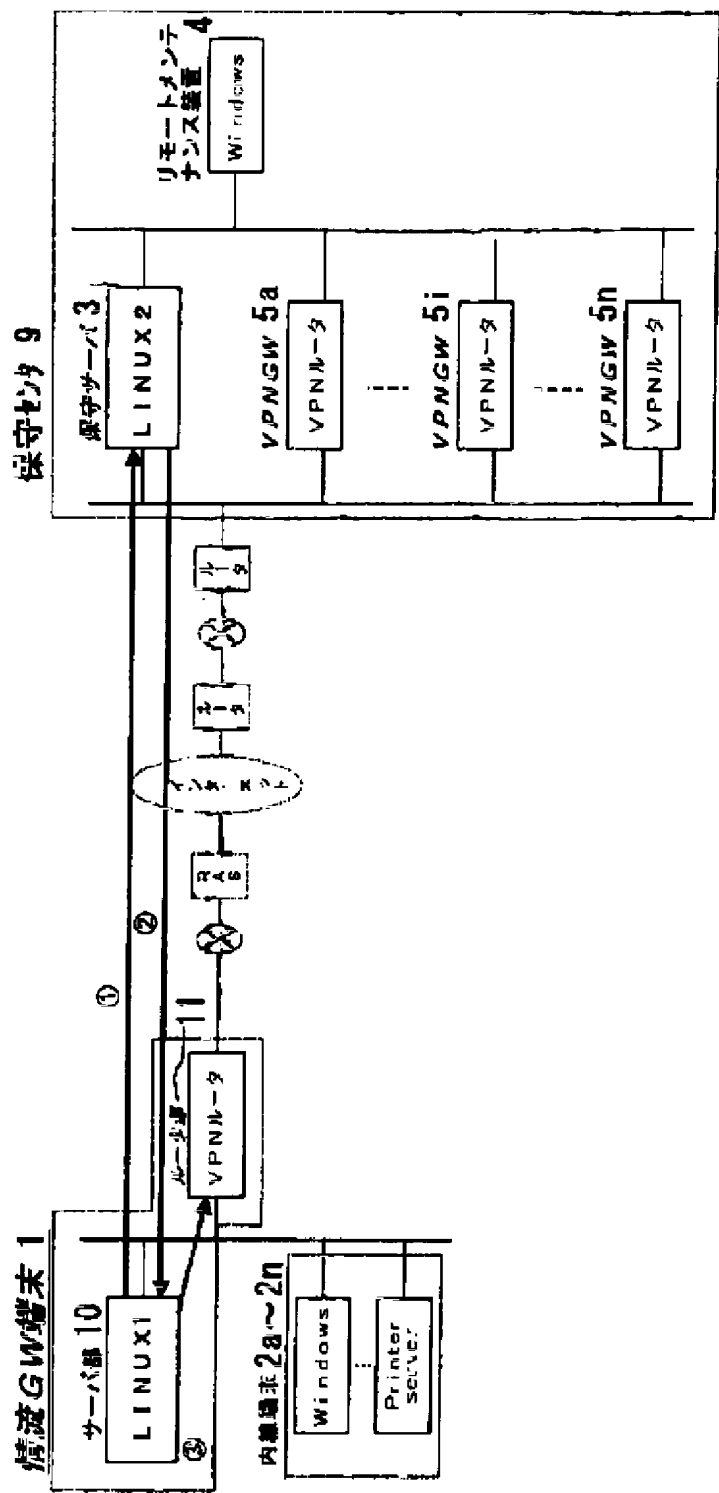
【図2】



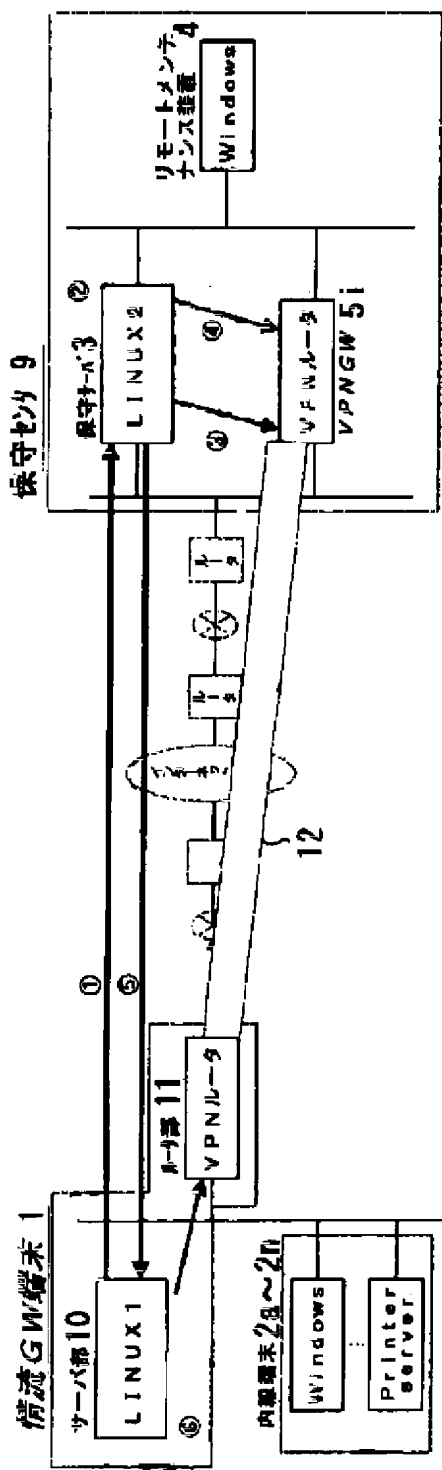
【図4】



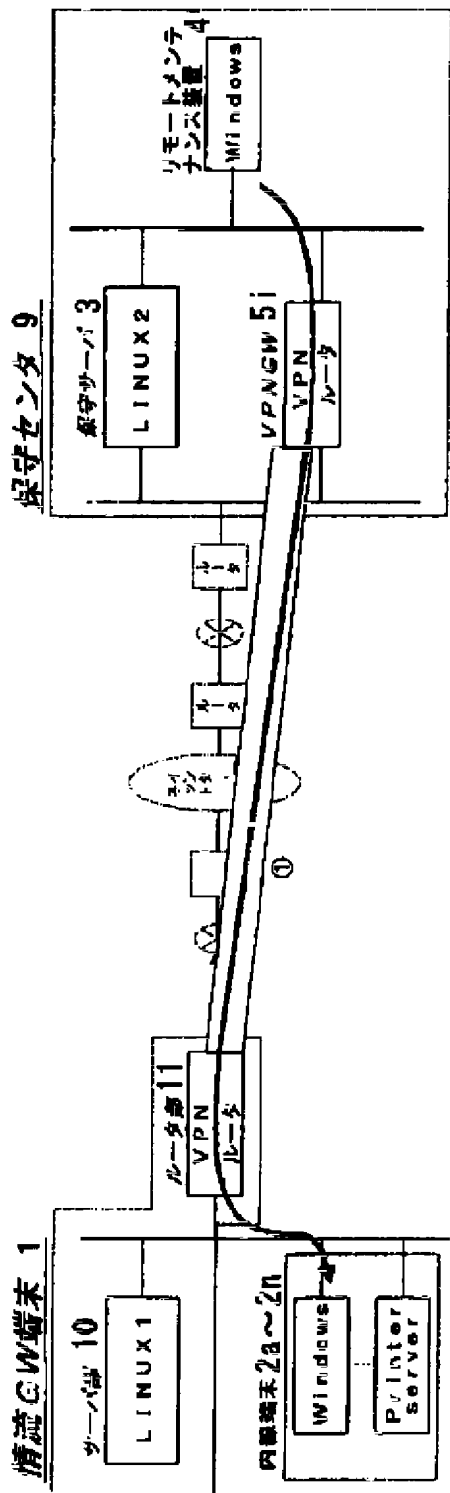
【図3】



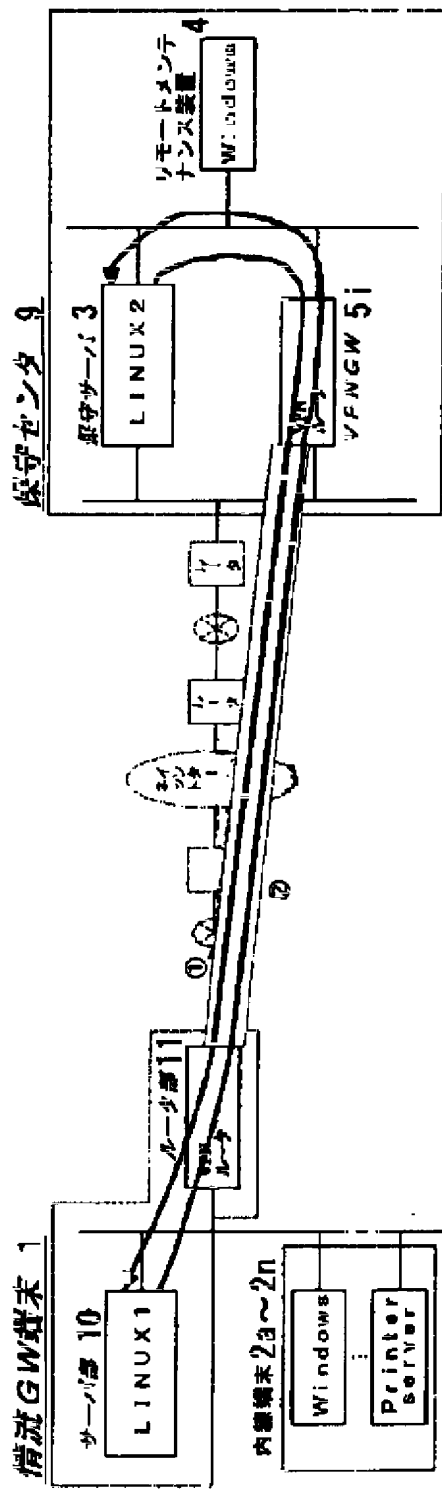
【図5】



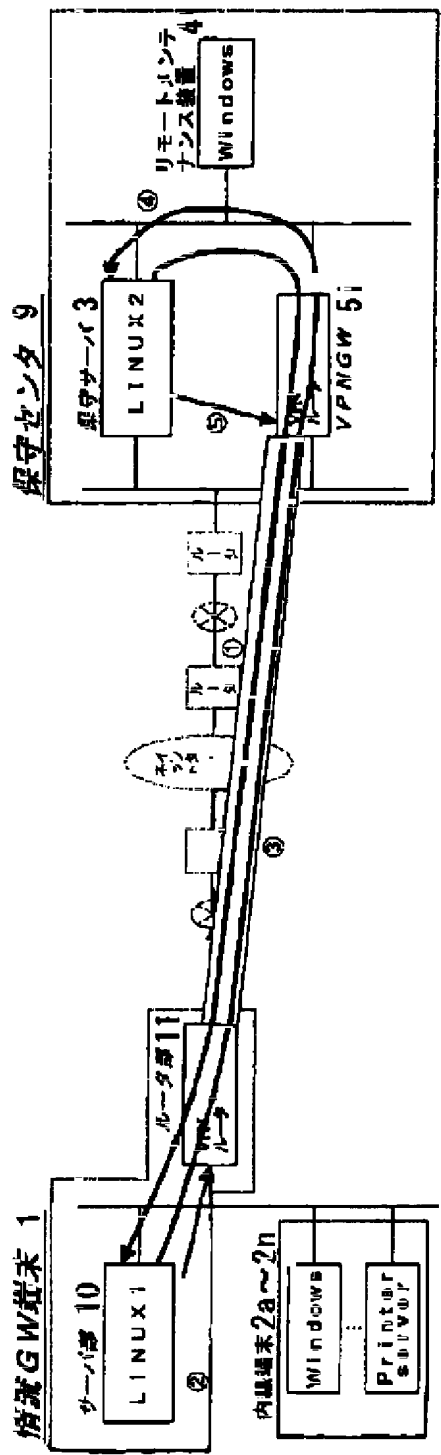
【図6】



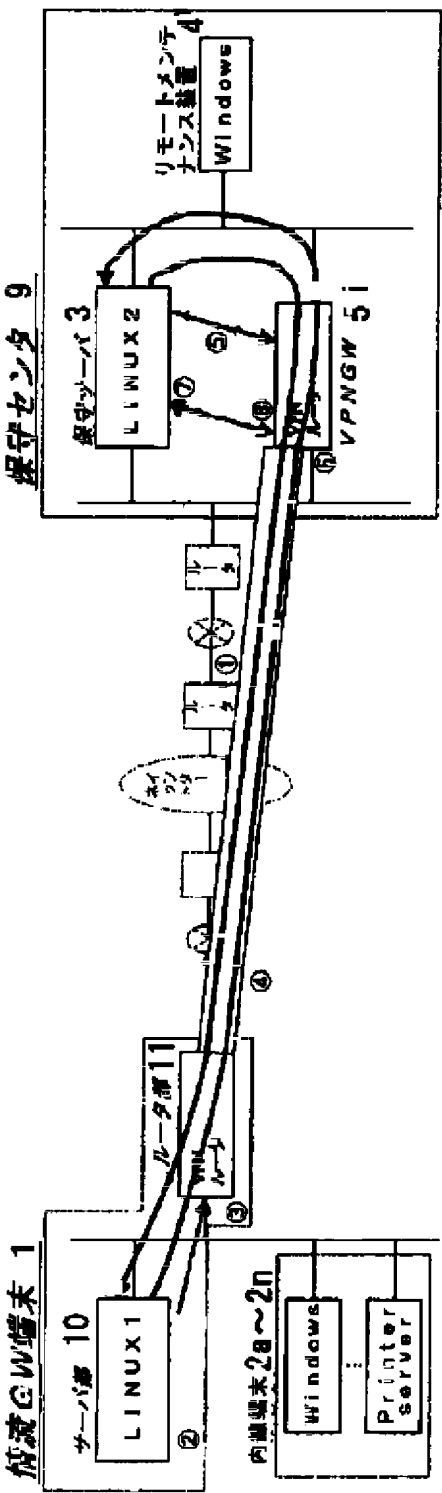
【図7】



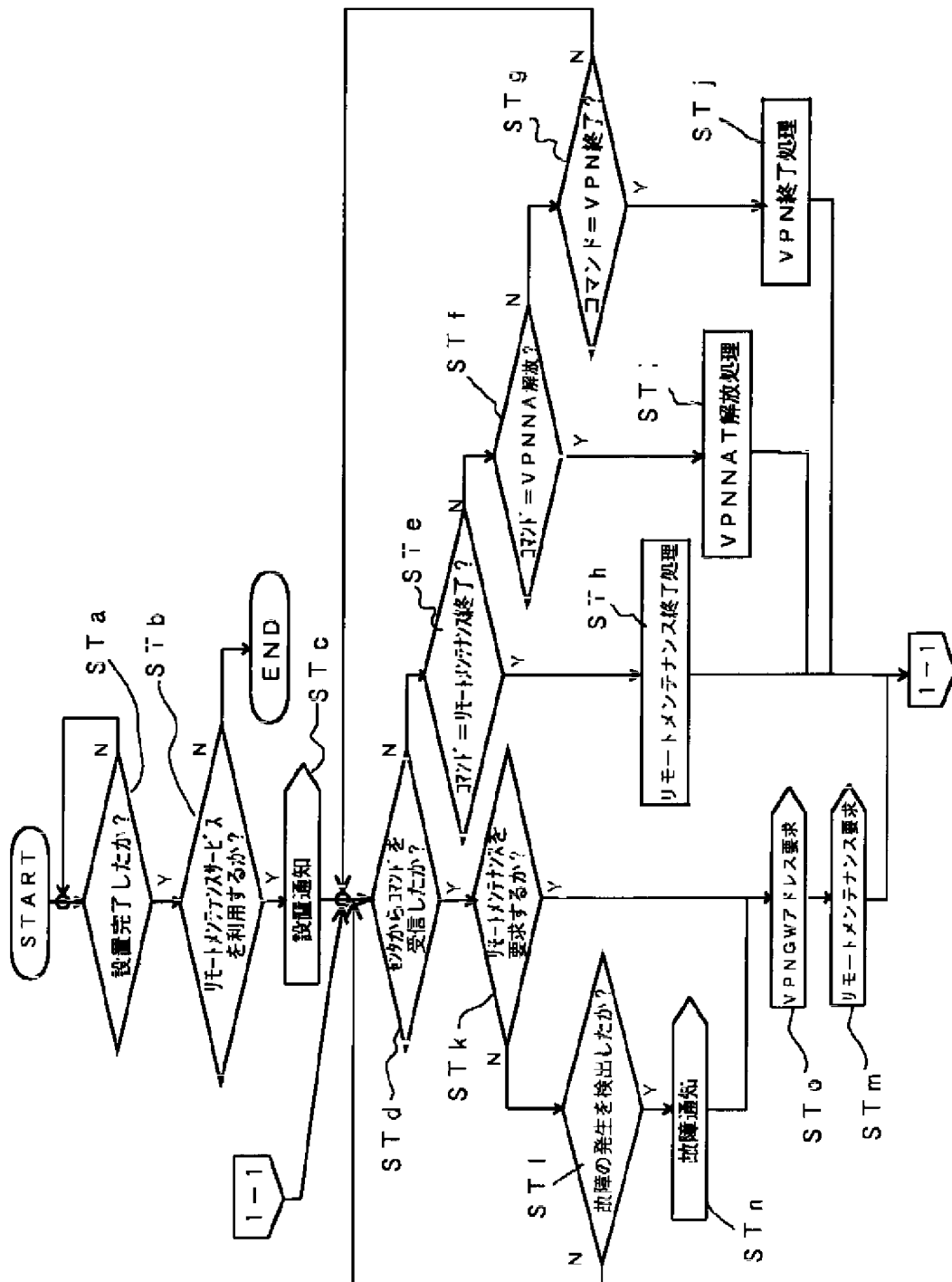
【図8】



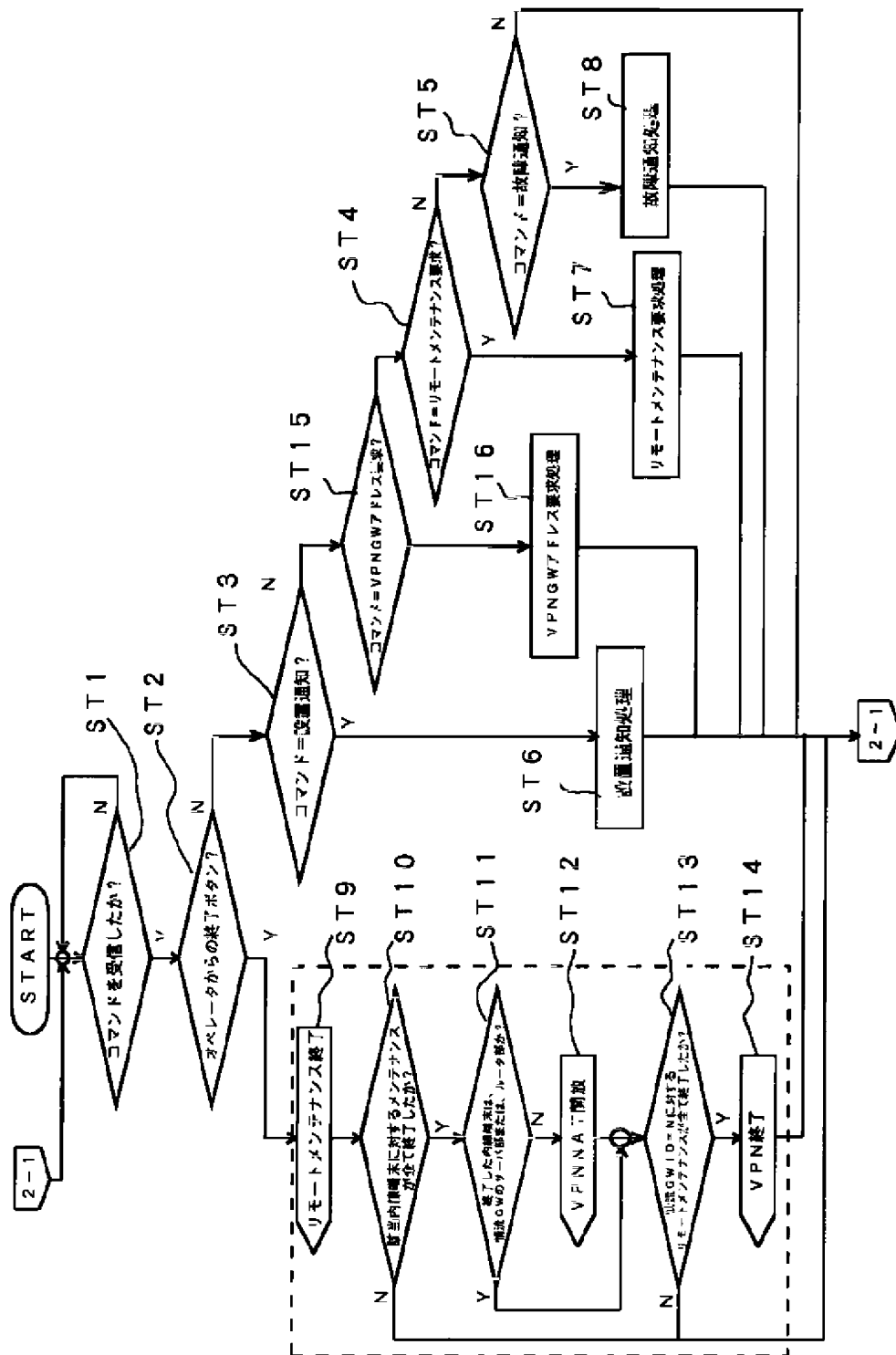
【図9】



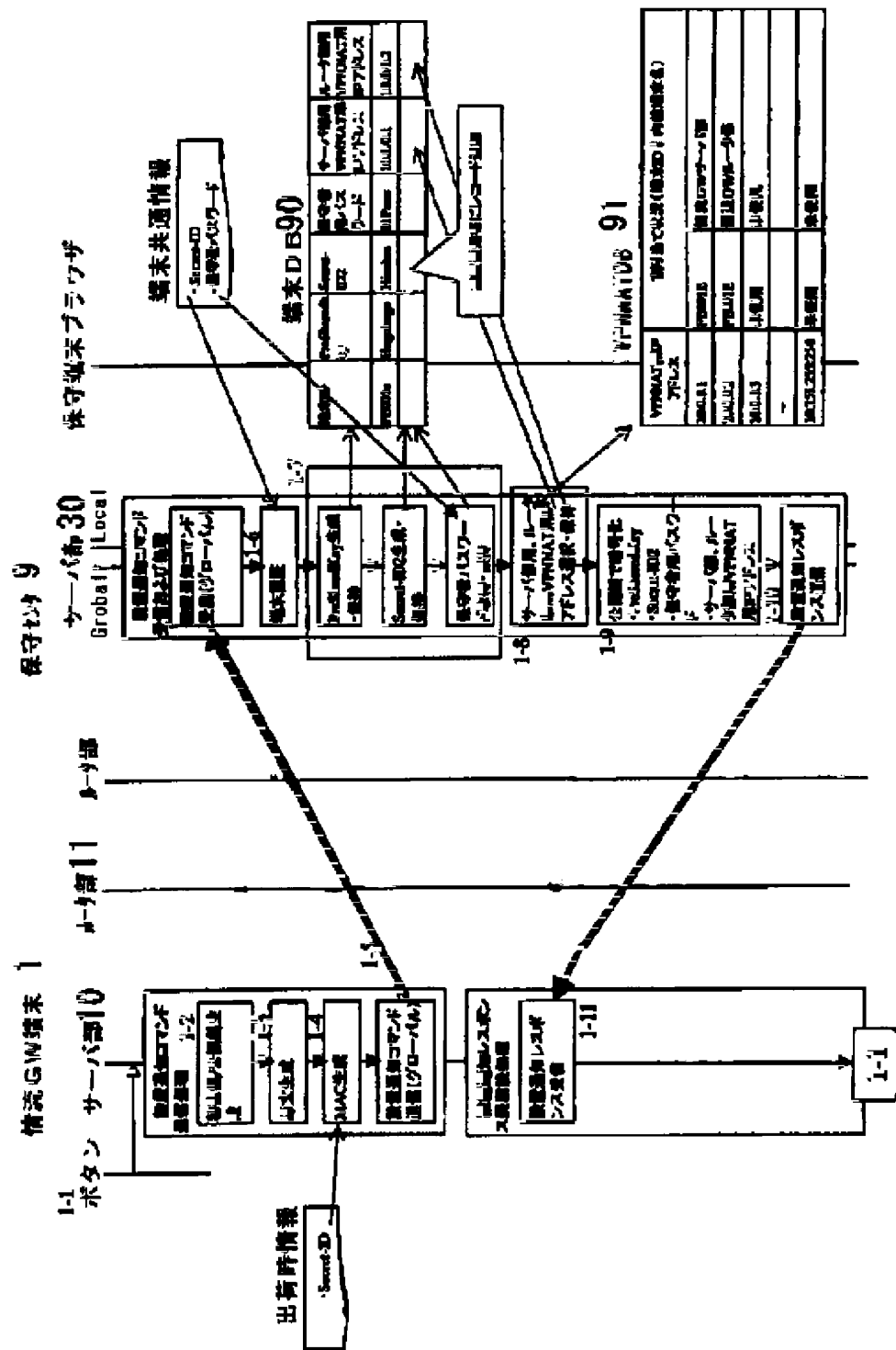
【☒ 10】

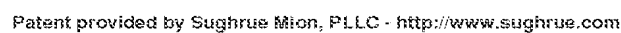


【図 1 1】

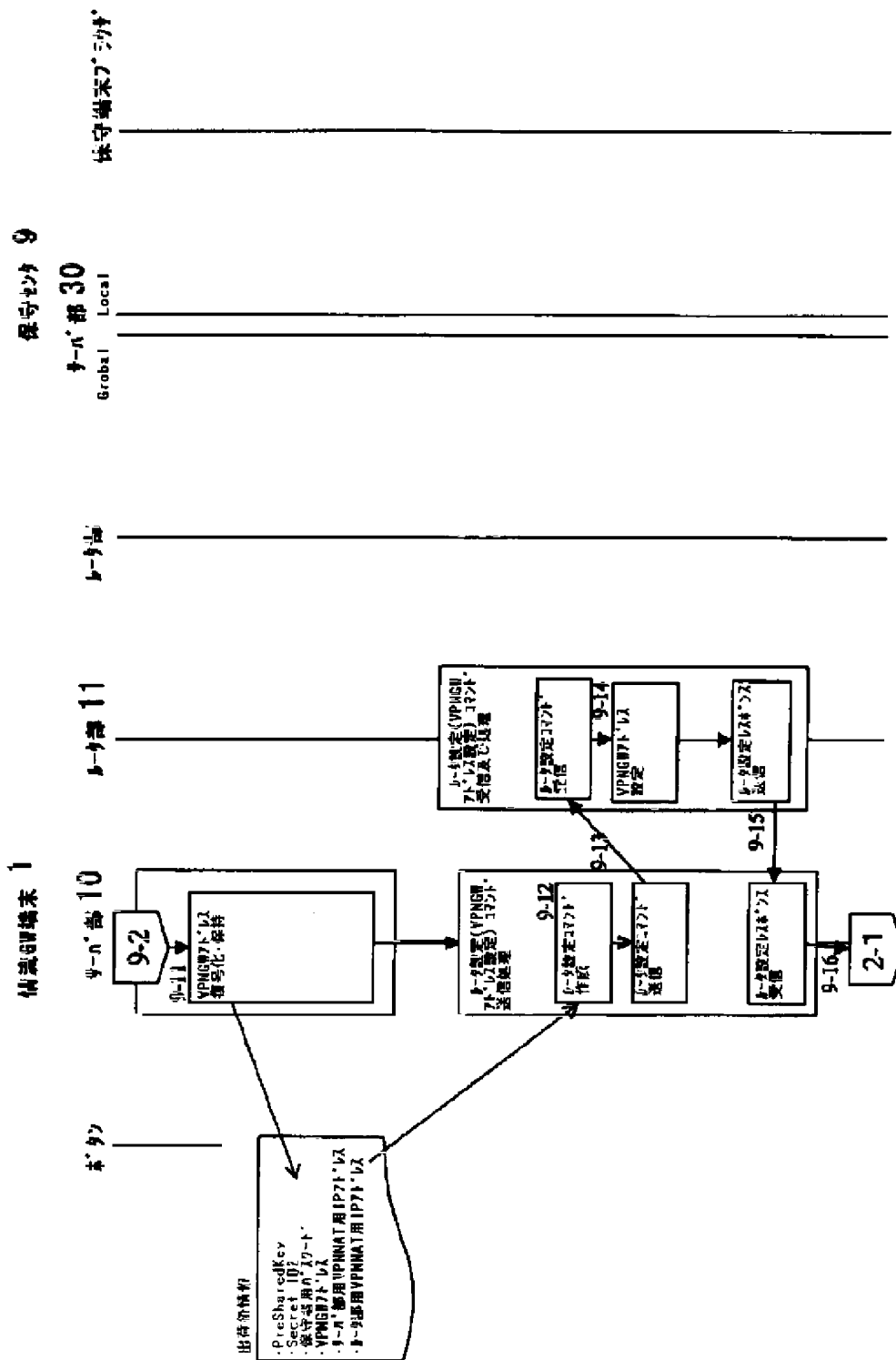


【図12】

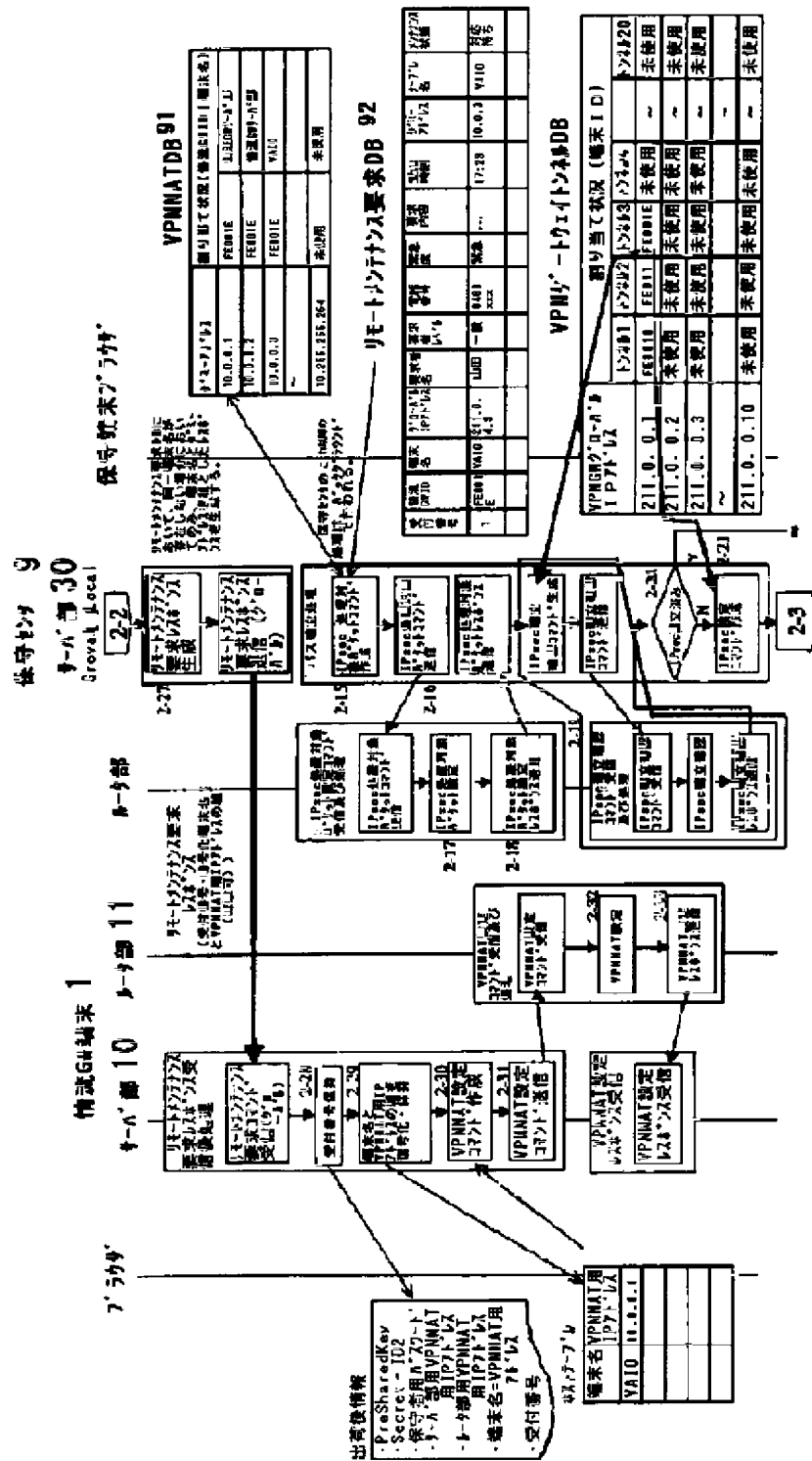




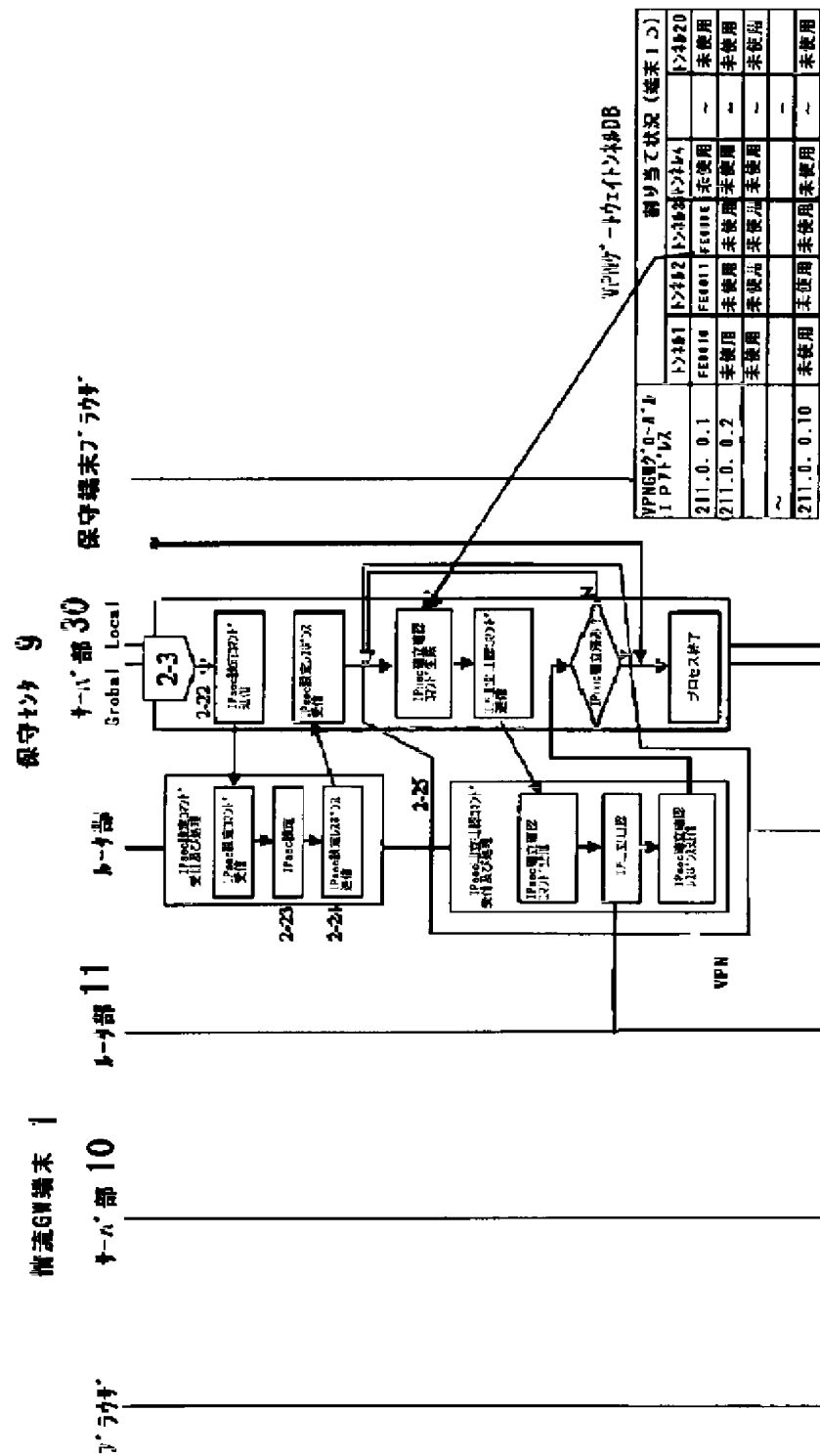
【例 15】



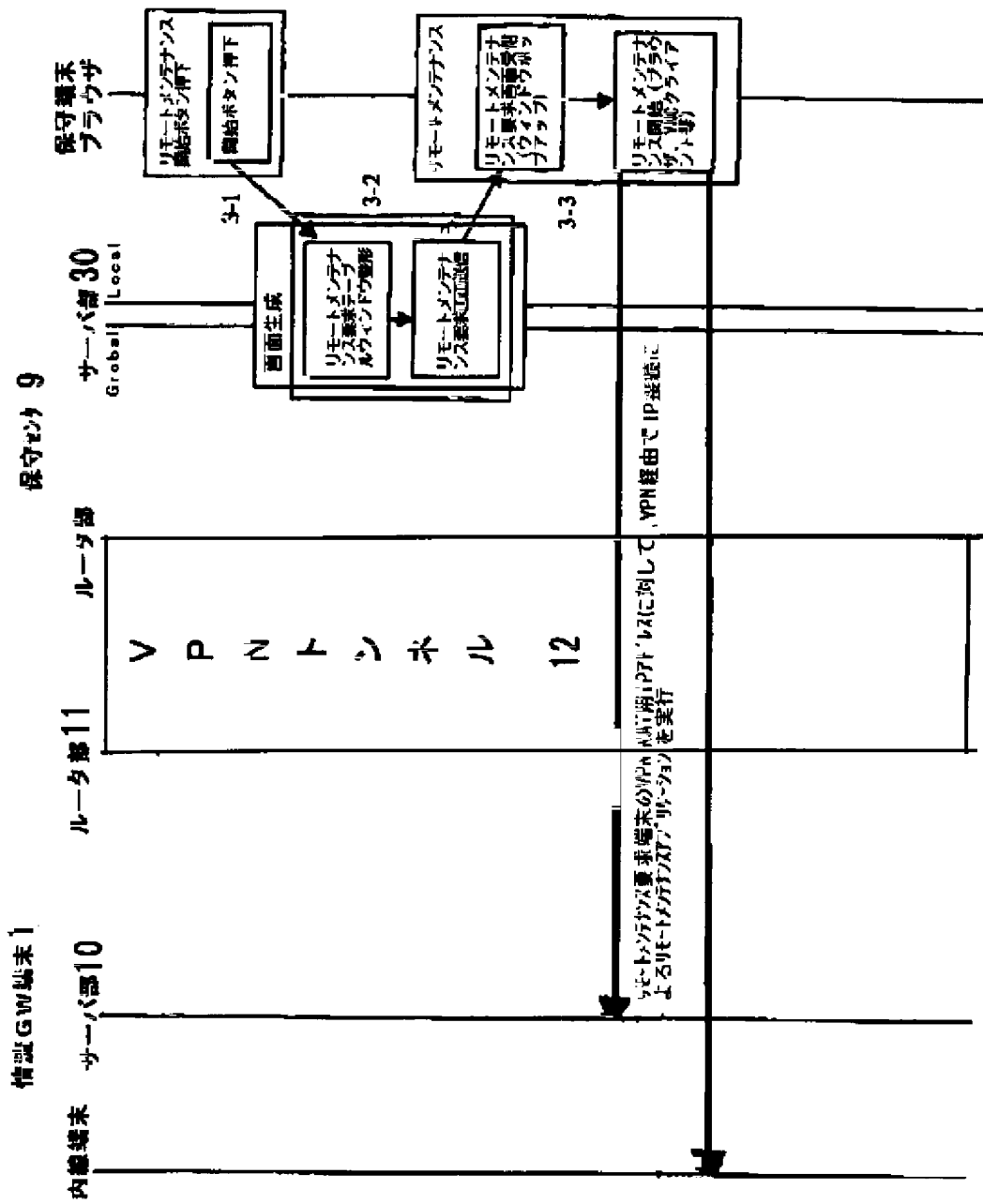
【図17】



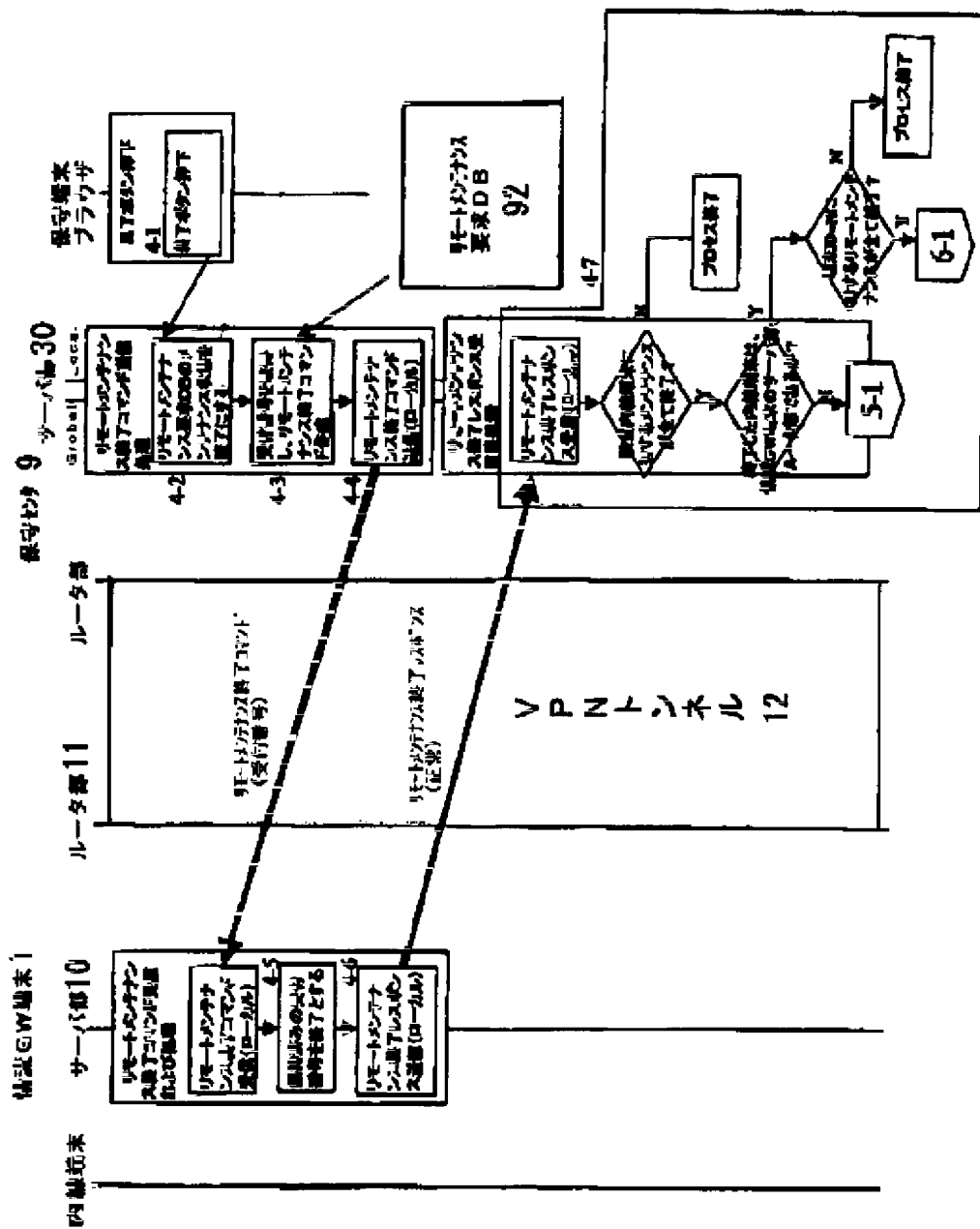
【例 18】



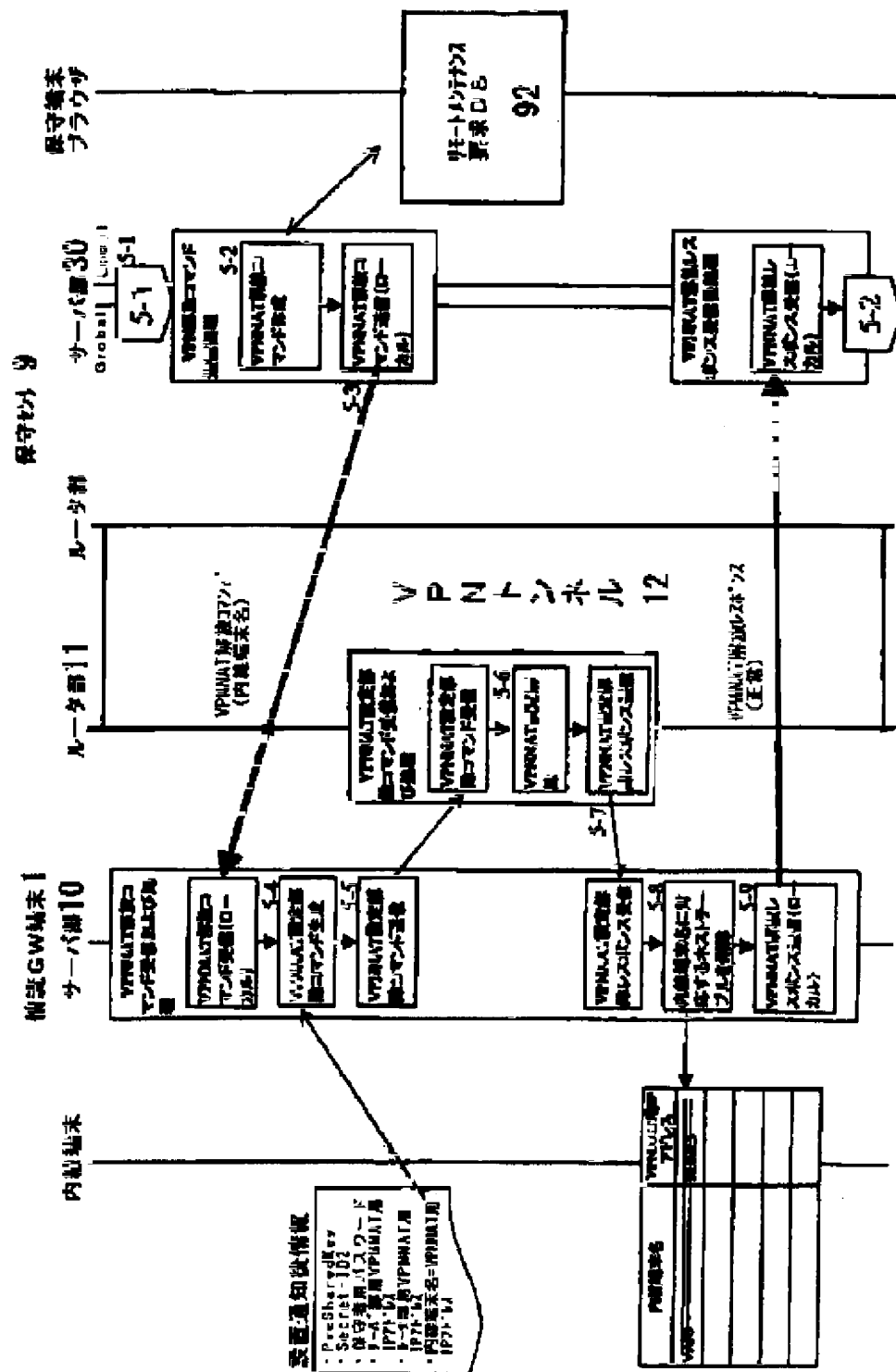
【図19】



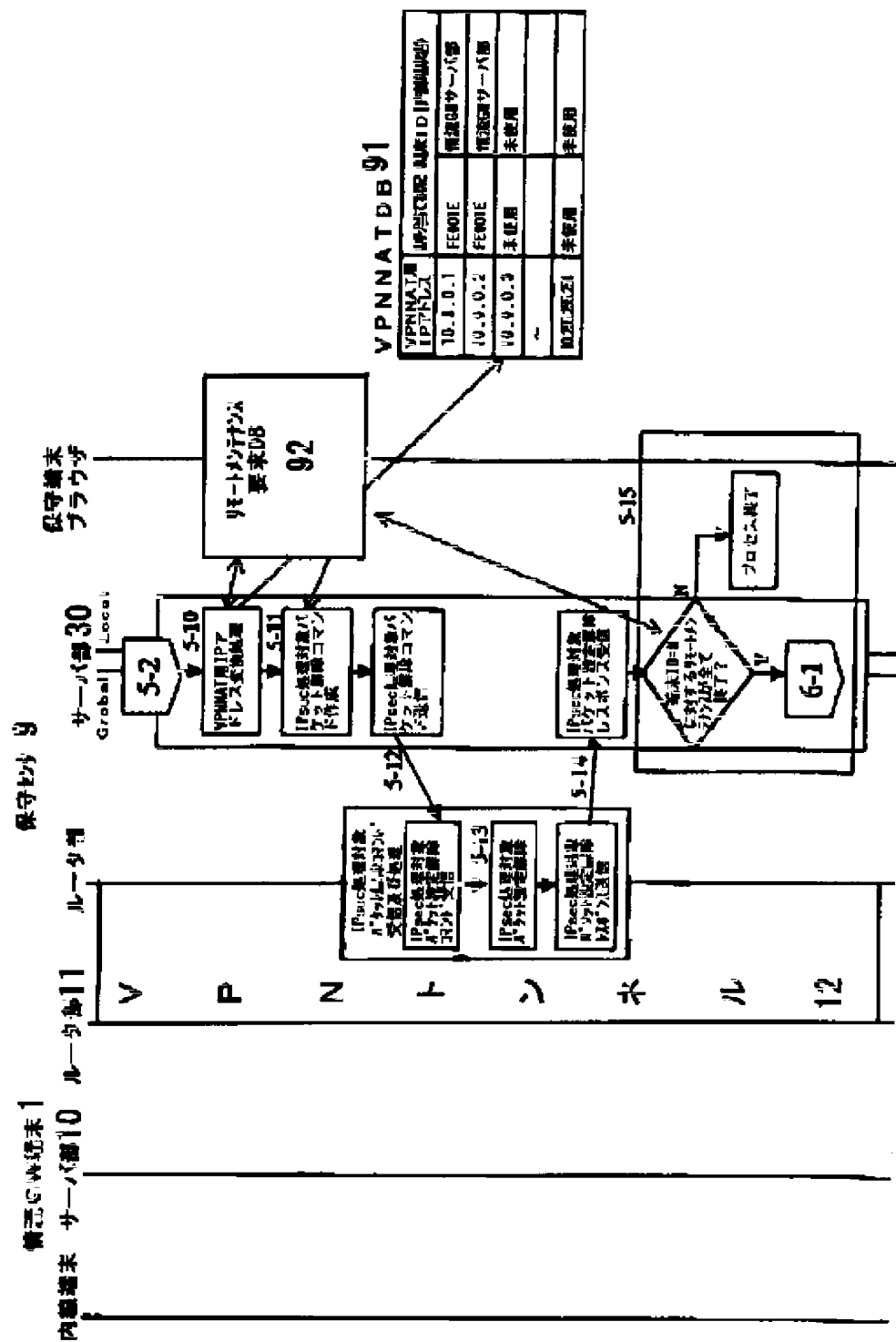
【図20】



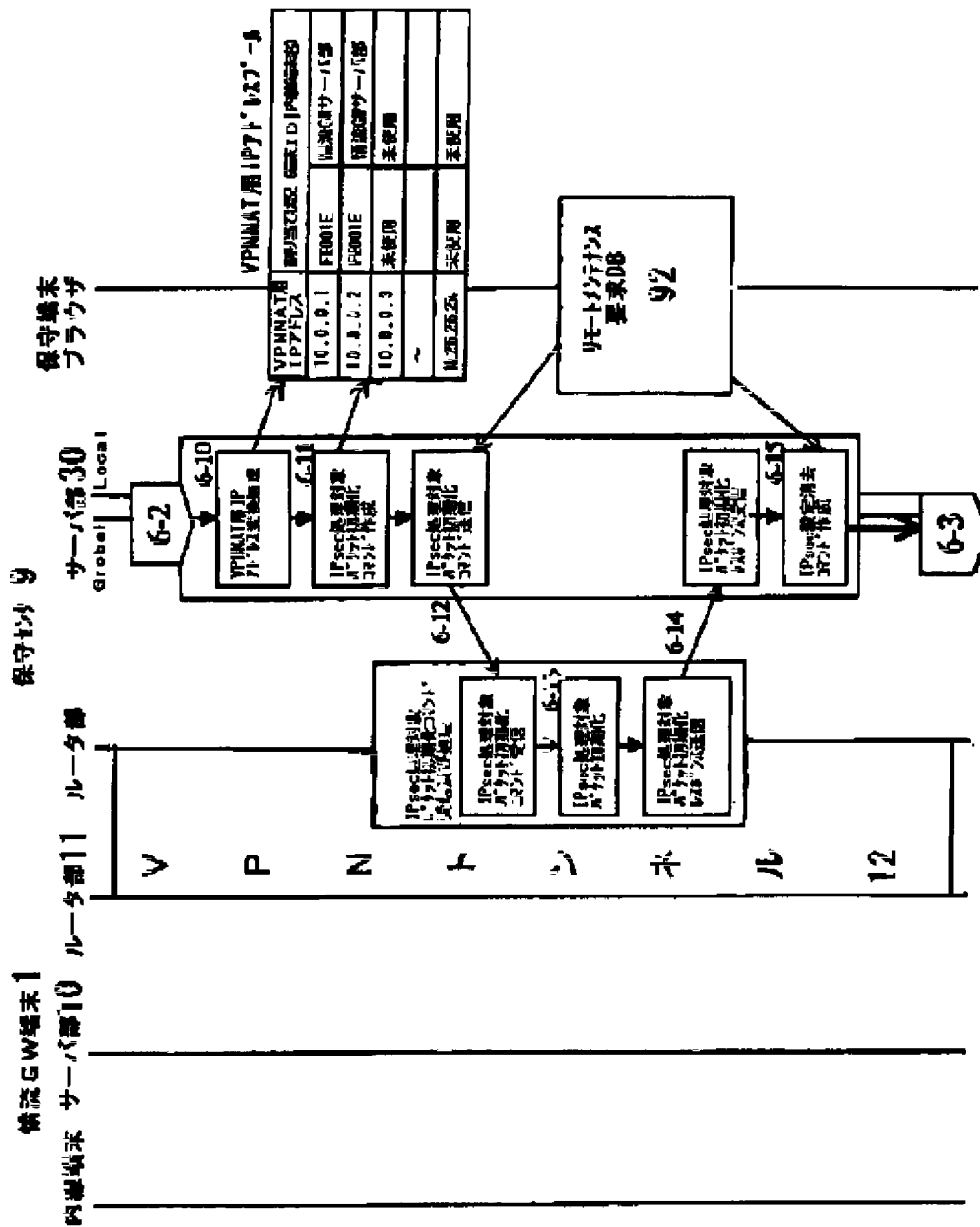
【例 2 1】



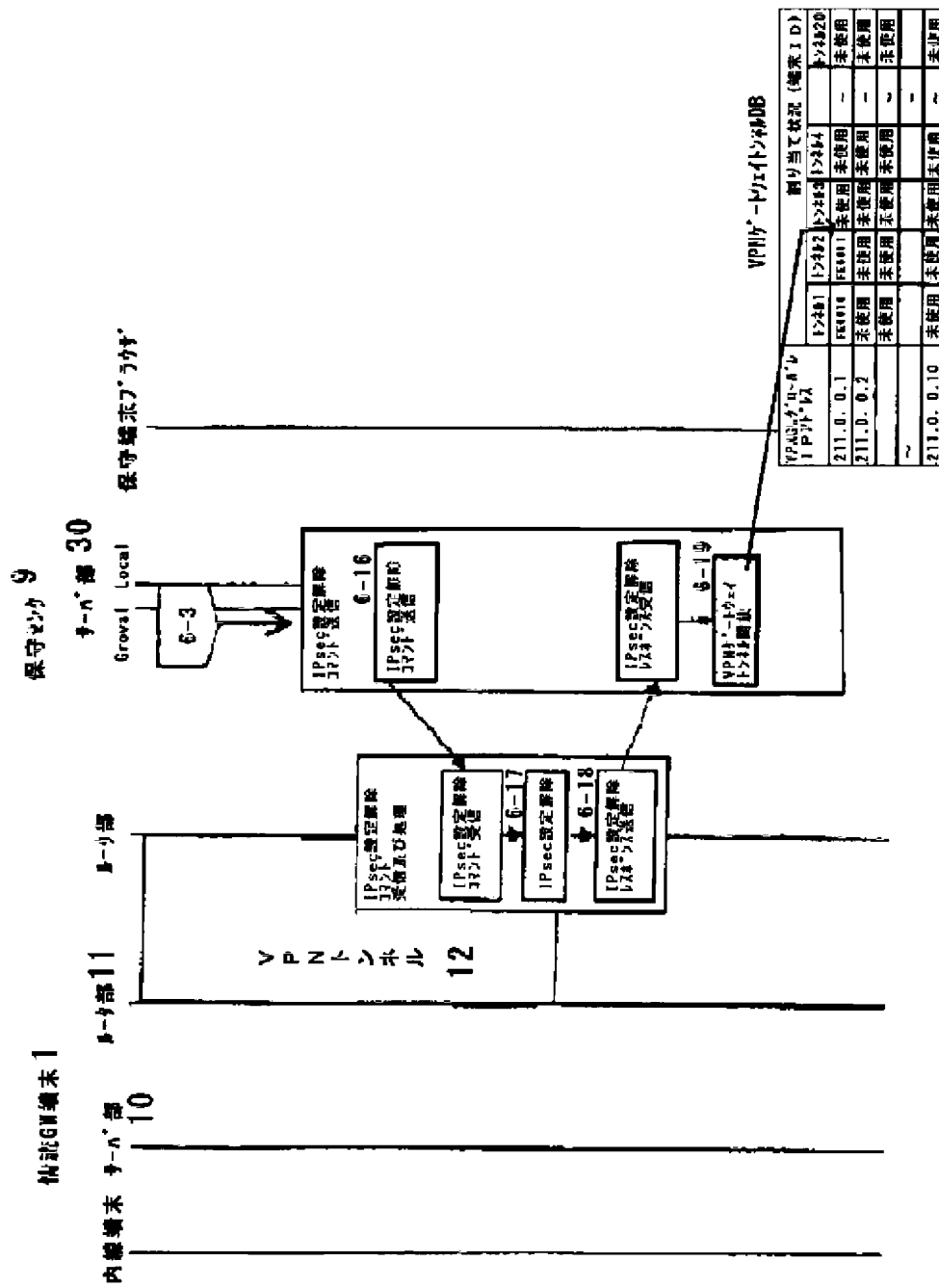
【例 22】



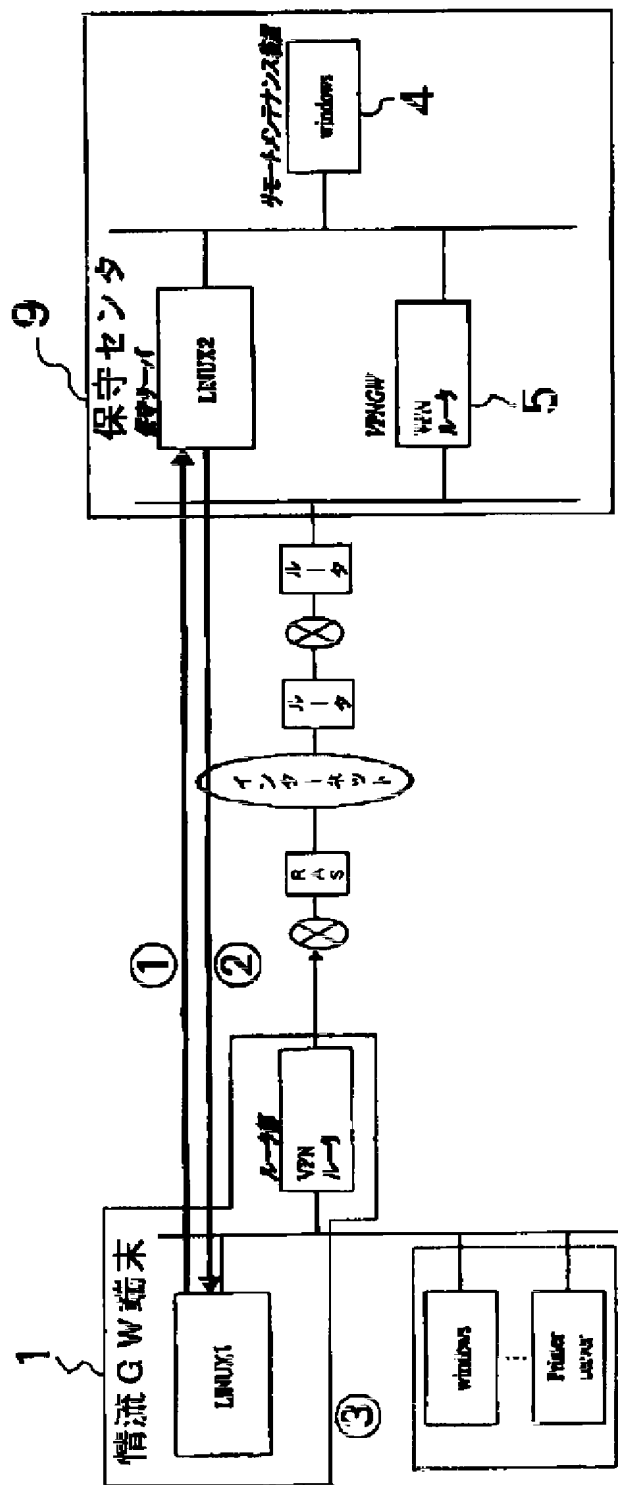
【图24】



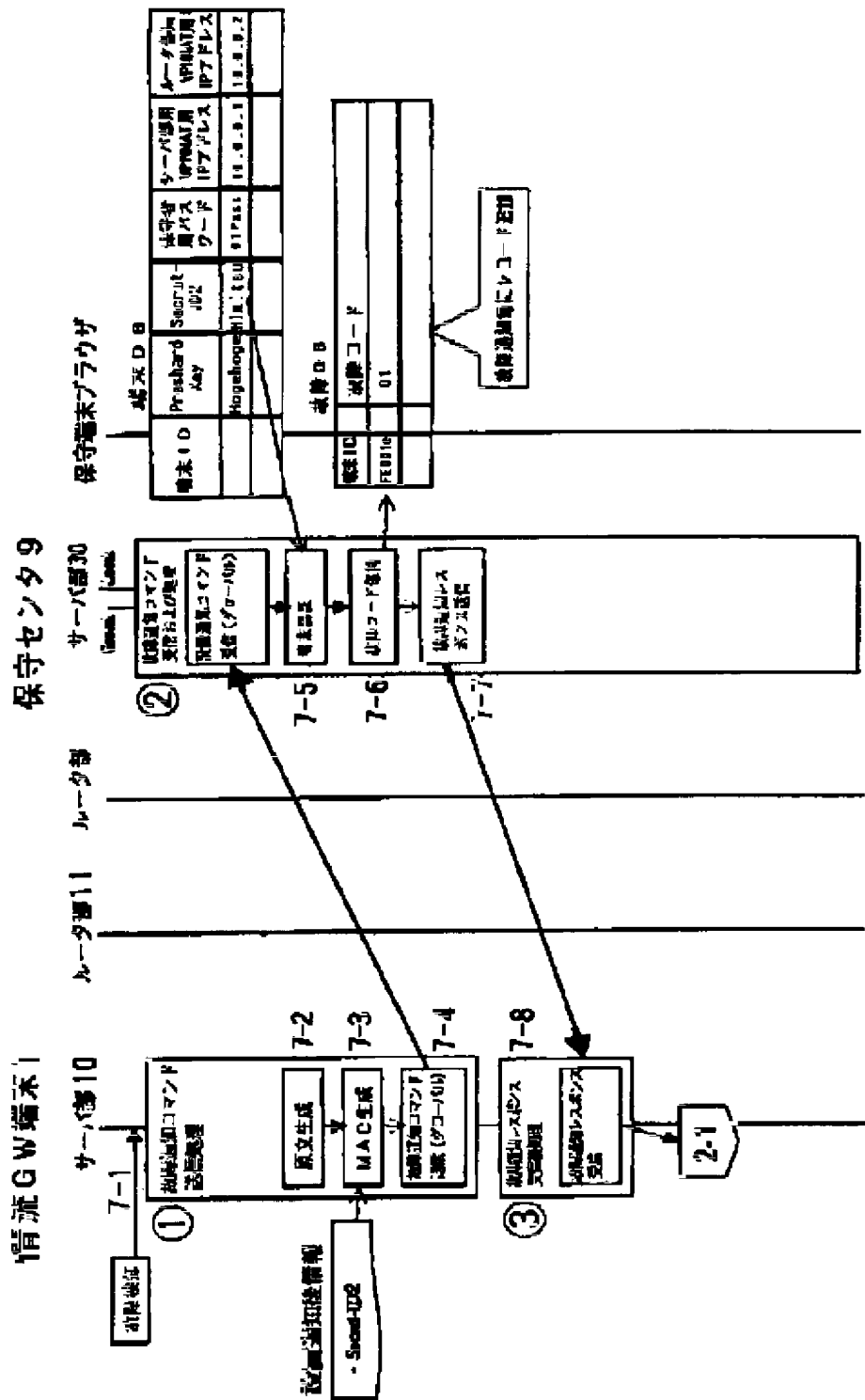
【例 25】



【図26】



【図27】



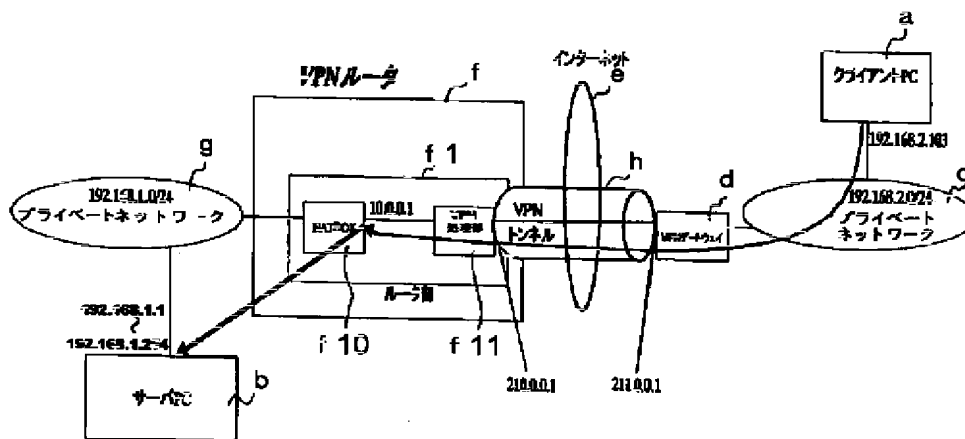
【図30】

VPN NAT DB 91		
VPN NAT 用 IP アドレス	割り当て状況 (端末 ID)	内線端末名
10.0.01	FE001E	情流 GW サーバ部
10.0.02	FE001E	情流 GW サーバ部
10.0.03	FE001E	VAIO
～		
10.255.255.254	未使用	未使用

【図31】

リモートメンテナンス要求DB 92												
受付 番号	端末 ID	内線 端末名	グローバル IPアドレス	要求 者名	要求者 レベル	電話番号	緊急度	要求 内容	受信 時刻	VPN/NAT 用 IP アドレス	テー ブル 名	メンテナ ンス 状態
1	FE001E	VAIO	211.0.4.3	山田	一般	0468xxx	緊急	---	17:23	10.0.03	VAIO	終了

【図32】



【図33】

